ON SOME PROBLEMS OF COMBINATORIAL NUMBER THEORY

by

Hugh Maxwell Wallace Edgar

DEPARTMENT OF MATHEMATICS

ABSTRACT

This thesis deals with some problems from the borderline of additive number theory and combinatorial analysis. In the first four chapters we give a survey of problems dealing with the separation of integers into (usually) non-overlapping classes satisfying certain conditions. The fifth chapter deals with problems on the addition chains of Scholz and Brauer while the last chapter is concerned with problems on representation of integers by distinct elements of certain sequences.

ON SOME PROBLEMS OF COMBINATORIAL NUMBER THEORY

by

Hugh Maxwell Wallace Edgar

Under the direction of

Dr. L. Moser

Department of Mathematics

University of Alberta

A THESIS

SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

Edmonton, Alberta. May, 1958.

ACKNOWLEDGEMENTS

I would like to extend my thanks to Dr. Leo Moser for his invaluable assistance in the preparation of this thesis.

TABLE OF CONTENTS

INTRODUCTION

In Chapter I we discuss a theorem due to Schur [30] and some related problems. More general results of Rado [21] are also discussed.

In Chapter II we consider two related topics: the first of these concerns a well-known theorem due to van der Waerden [33-36] while the second concerns "progression-free" sets. We discuss results due to Erdös and Rado [11], Moser [18], Behrend [1], Roth [23-25] and Varnivides [37] in connection with these problems.

In Chapter III we discuss two problems concerning finite sets of positive integers. In the first problem we separate the numbers 1, 2, ..., 2n into two disjoint classes $\tilde{A}$ and $\tilde{B}$, each class containing n numbers. The way in which we separate the numbers is, apart from the conditions stated, arbitrary. We investigate a property of the "difference set", defined to be the set of all integers (with multiplicities) which are obtained by subtracting an element of the class $\tilde{B}$ from an element of the class $\tilde{A}$. The second problem is the following: how many distinct positive integers not exceeding n can we have if we insist that all the possible sums, of one or more of these integers, be distinct?

In Chapter IV we consider problems of the following type: can every integer be represented as an element of one of a finite number of arithmetic progressions, each of whose common differences are distinct.

In Chapter V we consider a number of problems which arise in connection with the concept of "addition chains", introduced by Scholz [29]. The major portion of the chapter is an exposition

of a paper by Brauer [4], who solved some of the problems originally proposed by Scholz [29].

In Chapter VI we discuss some results due to Kelly [13] in connection with a problem concerning the possibility of representing positive integers as the sum of distinct elements of a given sequence.

CHAPTER I

<u>Introduction.</u> In this chapter we begin by discussing a result of Schur [30]. Schur proved that if sufficiently many positive consecutive integers $1, 2, \ldots, N(n)$ are separated into n classes in any manner whatsoever then at least one class contains elements x, y and z such that $x + y = z$. He made an application of his result to Fermat's last theorem. We end the chapter by discussing a more general theorem due to Rado [21].

Let us denote by $M(n)$ (assuming, for the moment, that it exists) the smallest number such that if $1, 2, 3, \ldots\ldots, M$ are separated into n classes in any manner whatsoever then at least one class contains elements x, y and z such that $x + y = z$.

We now proceed to obtain lower bounds for $M(n)$. Consider the numbers $1, 2, \ldots, (2^n-1)$. We separate these numbers by putting all the integers of the closed interval $[2^{k-1}, 2^k-1]$ in the kth class, $(1 \leq k \leq n)$. It is clear that no solutions of $x + y = z$ will be obtained in any class. In fact if we consider any two elements of the kth class, their sum is an element of the $(k + 1)$st class. If $n = 4$ we would obtain

1	2	4	8
(16)	3	5	9
(19)	(17)	6	10
(24)	(18)	7	11
(27)	(25)	(20)	12
	(26)	(21)	13
		(22)	14
		(23)	15

We see that it is possible to add more consecutive integers to this array without obtaining a solution. The numbers appearing in brackets are such numbers. Hence we can split more than (2^n-1)

numbers and still be without a solution. Thus $M(n) > (2^n-1)$. Alternately, we could write every integer m in the form $2^k \theta$ where θ is odd and put m in the kth class. If we have the elements $m_1 = 2^k \theta_1$ and $m_2 = 2^k \theta_2$ in the kth class then $(m_1 + m_2)$ must be an element of some rth class where r is greater than k and so we will obtain no solution in the kth class. With $n = 4$ we obtain

1	2	4	8
3	6	12	
5	10		
7	14		
9			
11			
13			
15			

We notice that in this case we cannot add any more integers without obtaining a solution.

We now prove that

$$(1.1) \qquad M(n) \geq \frac{(3^n - 1)}{2} + 1 = \frac{3^n + 1}{2} \quad .$$

The statement is trivially true for the case $n = 1$. We assume that it is possible to split the $\frac{3^k - 1}{2}$ numbers $1, 2, \ldots, \frac{(3^k - 1)}{2}$ into k classes without inducing any solutions and now prove that the $\frac{(3^{k+1} - 1)}{2}$ numbers $1, 2, \ldots, \frac{(3^{k+1} - 1)}{2}$ can be split into $(k + 1)$ classes without inducing a solution. We split the numbers as follows: the first $\frac{(3^k - 1)}{2}$ integers we arrange in k classes as in the case $n = k$. Any integer x such that

$$(1.2) \qquad \frac{(3^k - 1)}{2} + 1 \leq x \leq 2 \; \frac{(3^k-1)}{2} + 1$$

we put in the $(k+1)$st class. Finally, any integer y such that

$$(1.3) \qquad 2\,\frac{(3^k - 1)}{2} + 2 \leq y \leq \frac{(3^{k+1} - 1)}{2}$$

we place in the same class as the integer $y - \left(2\,\frac{(3^k - 1)}{2} + 1\right)$. In this way we certainly dispose of the required integers. It remains to show that there are no solutions of $x + y = z$ in any of the $(k+1)$ classes formed. It is obvious that there is no solution possible in the $(k+1)$st class. In the other k classes there are no solutions for integers not exceeding $\frac{(3^k - 1)}{2}$ by our induction hypothesis. Given any 3 y's in the range given by (1.2), say y_1, y_2 and y_3, it is not possible to have $y_1 + y_2 = y_3$ because of the restricted range of y. Also, the fact that y and $y - \left(2\,\frac{(3^k - 1)}{2} + 1\right)$ always occur in the same class means that the interval between any y_r and y_s must equal the interval between $x_r = y_r - \left(2\,\frac{(3^k - 1)}{2} + 1\right)$ and $x_s = y_s - \left(2\,\frac{(3^k - 1)}{2} + 1\right)$ so that we cannot obtain a solution of the type $x_r + y_s = y_t$. Finally, $x_r + x_s < y_t$ for all possible r, s and t. Hence we encounter no solutions in these first k classes. Thus the induction is complete.

We now show, in a different manner, that $M(n) \geq \frac{3^n + 1}{2}$. We use the base 3 and the 3 digits 1, 0 and -1 so that, for example, $15_{(10)}$ is represented as $1\text{-}1\text{-}10_{(3)}$ and $26_{(10)}$ is represented as $100\text{-}1_{(3)}$. Clearly the digit on the extreme left of any positive integer must be 1. The number of numbers having not more than n ternary digits is $1 + 3^1 + 3^2 + \ldots + 3^{n-1} = \frac{3^n - 1}{2}$. We separate these numbers as follows: if the first 1 appears in the rth place, counting from the digit on the extreme right of the number, we place the number in the rth class. It is easy to

show that no class can contain x, y and z such that $x + y = z$.

The two methods of showing that $M(n) \geq \frac{3^n + 1}{2}$ which have been discussed give rise to quite different arrays in the case $n = 4$. We exhibit these arrays, the array (1) being the result of the first method discussed.

(1)

1	2	5	14
4	3	6	15
10	11	7	16
13	12	8	17
28	29	9	18
31	30	32	19
37	38	33	20
40	39	34	21
		35	22
		36	23
			24
			25
			26
			27

(2)

1	2	5	14
4	3	6	15
7	11	8	17
10	12	9	18
13	20	32	23
16	21	33	24
19	29	35	26
22	30	36	27
25	38		
28	39		
31			
34			
37			
40			

Salié [28] has shown that $M(4) \geq 44$ by the following example:

1	2	4	5
7	3	10	6
12	9	11	8
15	14	13	17
18	22	16	20
21	30	19	24
23	35	25	27
26	41	28	36
29	42	31	38
32		33	39
37		34	
43		40	

Using the type of argument we employed to first show that $M(n) \geq \frac{3^n + 1}{2}$ we are now able to prove that

$$(1.4) \qquad M(n) \geq \frac{87}{162}\, 3^n + \frac{1}{2} \qquad \text{for} \quad n \geq 4$$

We now show that $M(2) = 5$ and $M(3) = 14$ so that $M(n) = \frac{(3^n - 1)}{2} + 1$ for these values of n. Clearly, the numbers 1 and 2 must be in different classes to avoid $1 + 1 = 2$. For $n = 2$ if 1 and 3 are in the same class, 4 can go in neither class. With 2 and 3 in the same class, 4 is forced into the same class as 1. The resulting array is optimal but the addition of 5 to either class now forces a solution. Let us now consider the case $n = 3$. We shall have 3 classes, which we denote by I, II and III. We can assume, without loss of generality, that 1 is

in

in I and 2 is II. If we have the $(r + s + t)$ numbers $a_1, a_2, \ldots, a_r$, $b_1, b_2, \ldots, b_s$, $c_1, c_2, \ldots, c_t$ separated so that the first r numbers are elements of class I, the next s numbers are elements of class II and the last t numbers are elements of class III and if such an array is solution-free we denote it by

$$\begin{array}{ccc} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_r & b_s & c_t \end{array}$$

. If in an array

$$\begin{array}{ccc} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_r & b_s & c_t \end{array}$$

the number x must be put in class I in order to maintain a solution-free array, we write

$$\begin{array}{ccc} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_r & b_s & c_t \end{array} \longrightarrow \begin{array}{ccc} a_1 & b_1 & c_1 \\ \cdot & & \\ \cdot & b_2 & c_2 \\ & \cdot & \cdot \\ a_r & \cdot & \cdot \\ x & b_s & c_t \end{array}$$

. We use similar notation if the class II or III is involved. If in an array

$$\begin{array}{ccc} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_r & b_s & c_t \end{array}$$

the number x forces a solution no matter

what class it is put in we write $\begin{array}{ccc} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_r & b_s & c_t \end{array}$: x. We construct all possible solution-free arrays involving the integers 1, 2 and 3 thus obtaining $1\ 2\ 3$, $\begin{array}{cc} 1 & 2 \\ & 3 \end{array}$ and $\begin{array}{cc} 1 & 2 \\ 3 & \end{array}$. We then append 4 in all possible solution-free ways, obtaining

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ & & 4 \end{array} , \quad \begin{array}{cc} 1 & 2 \\ 4 & 3 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ & 3 & \end{array} \quad \text{and} \quad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & & \end{array} .$$

Next we append 8. We now obtain

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 4 & & 8 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 8 & & 4 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ & 8 & 4 \end{array} , \quad \begin{array}{cc} 1 & 2 \\ 4 & 3 \\ & 8 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 8 \\ 4 & 3 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 8 & 3 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ & 3 & \\ & 8 & \end{array} ,$$

$$\begin{array}{ccc} 1 & 2 & 4 \\ 3 & & \\ 8 & & \end{array} \quad \text{and} \quad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & 8 & \end{array} .$$

Upon adding 5 in all possible solution-free ways, we get the possibilities

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & \\ & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 5 & & 4 \\ 8 & & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 8 & 5 & 4 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 8 & & 4 \\ & & 5 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 5 & 8 & 4 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ & 5 & 4 \\ & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ & 8 & 4 \\ & & 5 \end{array} ,$$

$$\begin{array}{ccc} 1 & 2 & 5 \\ 4 & 3 & \\ & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & 8 & 5 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 5 & 3 & \\ 8 & & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 8 & 3 & 5 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 5 & 3 & \\ & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ & 3 & 5 \\ & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & 5 & \\ 8 & & \end{array} ,$$

$$\begin{array}{ccc} 1 & 2 & 4 \\ 3 & & 5 \\ 8 & & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & 8 & \\ 5 & & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 4 \\ 3 & 5 & \\ & 8 & \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 8 & 5 \end{array} , \quad \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 8 \end{array} \quad \text{and} \quad \begin{array}{ccc} 1 & 2 & 5 \\ 4 & 3 & 8 \end{array} .$$

We now deal with these arrays individually

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & \\ & 8 & \end{array} \longrightarrow \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & \\ 6 & 8 & \end{array} \longrightarrow \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 10 \\ 6 & 8 & \end{array} : 7 .$$ Thus a solution is forced

by a number which does not exceed 14 and so the array $\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & \\ & 8 & \end{matrix}$

does not invalidate the statement $M(3) \leq 14$. We show that no other array invalidates the statement $M(3) \leq 14$ and that only the array $\begin{matrix} 1 & 2 & 5 \\ 4 & 3 & 8 \end{matrix}$ forces $M(3) = 14$.

$$\begin{matrix} 1 & 2 & 3 \\ 5 & & 4 \\ 8 & & \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 5 & 6 & 4 \\ 8 & & \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 5 & 6 & 4 \\ 8 & 7 & \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 5 & 6 & 4 \\ 8 & 7 & 8 \end{matrix} \quad : 13$$

$$\begin{matrix} 1 & 2 & 3 \\ 8 & 5 & 4 \end{matrix} \quad : 7$$

$$\begin{matrix} 1 & 2 & 3 \\ 8 & & 4 \\ & & 5 \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 8 & 7 & 4 \\ & & 5 \end{matrix} \quad : 9$$

$$\begin{matrix} 1 & 2 & 3 \\ 5 & 8 & 4 \end{matrix} \quad : 6$$

$$\begin{matrix} 1 & 2 & 3 \\ & 5 & 4 \\ & 8 & \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 6 & 5 & 4 \\ & 8 & \end{matrix} \quad : 7$$

$$\begin{matrix} 1 & 2 & 3 \\ & 8 & 4 \\ & & 5 \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 6 & 8 & 4 \\ & & 5 \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 6 & 8 & 4 \\ & 7 & 5 \end{matrix} \to \begin{matrix} 1 & 2 & 3 \\ 6 & 8 & 4 \\ 9 & 7 & 5 \end{matrix} \quad : 10$$

$$\begin{matrix} 1 & 2 & \\ 4 & 3 & 5 \\ & 8 & \end{matrix} \to \begin{matrix} 1 & 2 & 5 \\ 4 & 3 & 6 \\ & 8 & \end{matrix} \to \begin{matrix} 1 & 2 & 5 \\ 4 & 3 & 6 \\ 10 & 8 & \end{matrix} \quad : 11$$

$$\begin{matrix} 1 & 2 & 4 \\ 3 & 8 & 5 \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 3 & 8 & 5 \\ 10 & & \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 3 & 8 & 5 \\ 10 & & 6 \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 3 & 8 & 5 \\ 10 & 9 & 6 \end{matrix} \quad : 11$$

$$\begin{matrix} 1 & 2 & 4 \\ 5 & 3 & \\ 8 & & \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 5 & 3 & 6 \\ 8 & & \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 5 & 3 & 6 \\ 8 & 10 & \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 5 & 3 & 6 \\ 8 & 10 & 7 \end{matrix} \quad : 13$$

$$\begin{matrix} 1 & 2 & 4 \\ 8 & 3 & 5 \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 8 & 3 & 5 \\ & 9 & \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 8 & 3 & 5 \\ & 9 & 7 \end{matrix} \to \begin{matrix} 1 & 2 & 4 \\ 8 & 3 & 5 \\ 11 & 9 & 7 \end{matrix} \quad : 12$$

$$\begin{array}{ccc}1&2&4\\5&3&\\&8&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\5&3&6\\&8&\end{array} \quad : 10$$

$$\begin{array}{ccc}1&2&4\\&3&5\\&8&\end{array} \longrightarrow \begin{array}{cccc}&1&2&4\\10&3&5&\\&8&&\end{array} \longrightarrow \begin{array}{cccc}&1&2&4\\10&3&5&\\&8&11&\end{array} \longrightarrow \begin{array}{cccc}&1&2&4\\10&3&5&\\6&8&11&\end{array} \quad : 7$$

$$\begin{array}{ccc}1&2&4\\3&5&\\8&&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&7\\8&&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&7\\8&11&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&7\\8&11&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&7\\8&11&9\\&&6\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&7\\8&11&9\\10&&6\end{array} \quad : 13$$

$$\begin{array}{ccc}1&2&4\\3&&5\\8&&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&9&5\\8&&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&9&5\\8&&7\end{array} \quad : 11$$

$$\begin{array}{ccc}1&2&4\\3&8&\\5&&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&8&6\\5&&\end{array} \quad : 10$$

$$\begin{array}{ccc}1&2&4\\3&5&\\&8&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&6\\&8&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&6\\10&8&\end{array} \longrightarrow \begin{array}{ccc}1&2&4\\3&5&6\\10&8&7\end{array} \quad : 13$$

$$\begin{array}{ccc}1&2&3\\4&8&5\end{array} \longrightarrow \begin{array}{ccc}1&2&3\\4&8&5\\6&&\end{array} \quad : 10$$

The array $\begin{array}{ccc}1&2&3\\4&5&8\end{array}$ results in 2 possible arrays

$$\begin{array}{ccc}1&2&3\\4&5&8\\10&&\end{array} \quad \text{and} \quad \begin{array}{ccc}1&2&3\\4&5&8\\&&10\end{array} \quad .$$

$$\begin{array}{ccc}1&2&3\\4&5&8\\10&&\end{array} \longrightarrow \begin{array}{ccc}1&2&3\\4&5&8\\10&6&\end{array} \quad : 11 \quad \text{and} \quad \begin{array}{ccc}1&2&3\\4&5&8\\&&10\end{array} \longrightarrow \begin{array}{ccc}1&2&3\\4&5&8\\7&&10\end{array} \longrightarrow \begin{array}{ccc}1&2&3\\4&5&8\\7&6&10\end{array} \quad : 11 \; .$$

Finally the array $\begin{array}{ccc}1&2&5\\4&3&8\end{array}$ also results in 2 possible arrays,

$$\begin{array}{ccc}1&2&5\\4&3&8\\6&&\end{array} \quad \text{and} \quad \begin{array}{ccc}1&2&5\\4&3&8\\&&6\end{array} \quad .$$

$$\begin{matrix}1&2&5\\4&3&8\\6&&\end{matrix} \longrightarrow \begin{matrix}1&2&5\\4&3&8\\6&10&\end{matrix} \longrightarrow \begin{matrix}1&2&5\\4&3&8\\6&10&7\end{matrix} \qquad : 12$$

$$\begin{matrix}1&2&5\\4&3&8\\&&6\end{matrix} \longrightarrow \begin{matrix}1&2&5\\4&3&8\\10&11&6\\13&12&9\end{matrix} \qquad : 14$$ where 7 may be put in any class.

Hence $M(3) = 14$ and there are exactly 3 ways of separating the numbers $1, 2, \ldots, 13$ into 3 classes so that we have a solution-free array.

We now state and prove the theorem due to Schur [30].

THEOREM 1.1:

If the consecutive positive integers $1,2,3, \ldots [n!e]$ are separated into n classes in any manner whatsoever then at least one class will contain elements x,y and z such that $x + y = z$. ($[x]$ denotes the integral part of x)

PROOF:

We define

$$(1.5) \qquad T_0 = 1, \quad T_n = n\, T_{n-1} + 1 \quad \text{for} \quad n \geq 1 .$$

We then have

$$T_n = n\, T_{n-1} + 1 = n\,((n-1)\, T_{n-2} + 1) + 1 = n(n-1)\, T_{n-2} + n + 1$$

$$T_n = n(n-1)((n-2)\, T_{n-3} + 1) + n+1 = n(n-1)(n-2)\, T_{n-3} + n(n-1) + n + 1$$

Continuing in this way, we see that

$$T_n = n(n-1)\ldots(n-(n-1))\, T_{n-(n)} + n(n-1)\ldots(n-(n-2))+\ldots+n(n-1) + n + 1$$

$$T_n = n! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{(n-1)!} + \frac{1}{n!}\right) .$$

+ sign

Now $n!\, e = n! \sum_{r=o}^{\infty} \frac{1}{r!} = n! \left(\frac{1}{0!} + \frac{1}{1!} + \dots + \frac{1}{n!}\right) + n!\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots\right.$

$$n!\, e = T_n + n! \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots\right) .$$

Further, $n! \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots\right) < \frac{n!}{(n+1)!} \left(1 + \frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \dots\right.$

Hence $n! \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots\right) < \frac{1}{(n+1)} \frac{n+1}{n} = \frac{1}{n}$

Hence $n! \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots\right) < 1$ for all $n \geq 1$.

Thus we have $T_n < n!e < T_n + 1$ and therefore

(1.6) $\quad T_n = [n!e]$.

We now assume that the numbers $1, 2, \dots T_n$ have been separated in such a manner as to yield no solution of $x + y = z$ in any class and from this assumption obtain a contradiction. In order that $x + y \neq z$ it must be the case that no class can contain the difference of 2 of its elements. Generally, if we have some class A containing t elements $a_1 < a_2 < \dots < a_t$ then we may form the $(t-1)$ distinct "first differences" $b_1 = a_2 - a_1$, $b_2 = a_3 - a_1$, $\dots$ $b_{t-1} = a_t - a_1$. These "first differences" cannot lie in A . We may also form $(t-2)$ distinct "second differences"
$c_1 = b_2 - b_1$, $c_2 = b_3 - b_1$, $\dots$ $c_{t-2} = b_{t-1} - b_1$. These elements cannot be in the class A either because they also are differences of the original elements of A. In our case,

we begin with T_n elements. Hence we must have at least $\frac{T_n}{n}$ elements in some one of our n classes, say A_1. Now

$$\frac{T_n}{n} = \frac{n\,T_{n-1} + 1}{n} = T_{n-1} + \frac{1}{n}$$ but the number of elements in A_1 must be integral so that we must have at least $T_{n-1} + 1 = \left[\frac{T_n}{n} + 1\right]$ elements in A_1. We now form the T_{n-1} distinct "first differences". These elements cannot lie in A_1 and so must be distributed among the remaining $(n-1)$ classes. Hence in some class, say A_2, we must have at least $\left[\frac{T_{n-1}}{n-1} + 1\right] = T_{n-2} + 1$ elements. Once again, we form differences, producing T_{n-2} elements, the c's, which cannot be in either A_1 or A_2. Continuing in this manner, we eventually obtain $T_0 = 1$ elements which cannot belong to any one of the classes $A_1, A_2, \ldots, A_n$. However, this element must, due to the method of construction, be one of the numbers $1, 2, \ldots, T_n$. Hence we have a contradiction.

We now have $M(n) \geq \frac{3^n + 1}{2}$ for $n \geq 1$, $M(n) \geq \frac{87}{162}\, 3^n + \frac{1}{2}$ for $n \geq 4$ and $M(n) \leq [n!e]$ for $n \geq 1$.

We list the values of these functions obtained for the first few values of n.

n	$\frac{3^n+1}{2}$	$\frac{87}{162}\, 3^n + \frac{1}{2}$	$[n!e]$	$M(n)$
1	2		2	2
2	5		5	5
3	14		16	14
4	41	44	65	?
5	122	131	326	?

It is clear that $[n!e]$ will be much larger than $\frac{87}{162}\, 3^n + \frac{1}{2}$

when n becomes large. However, it is not known whether $[n!e]$ can be replaced by some quantity which will be considerably smaller than $[n!e]$ for sufficiently large n.

We should now like to consider certain questions which are closely related to Schur's theorem. In the proof of the theorem it was shown that it was sufficient to take T_n consecutive positive integers in order to obtain a contradiction. We should now like to approach the question somewhat differently in order to determine the reason for choosing the number T_n. Let us now assume that we have the numbers $1, 2, \ldots, B_n$ where B_n is taken to be some number which is sufficiently large to force at least one solution of $x + y = z$ in at least one of the classes. We may write $B_n = \alpha_1 n + \beta_1$, where α_1 is a positive integer and where we must have $0 \leq \beta_1 \leq (n-1)$. Let us assume, for the time being, that $\beta_1 \geq 1$. We proceed with the argument used in the proof of Schur's theorem. We must have at least $\left[\frac{B_n}{n} + 1\right]$ elements in some class A_1 because $\beta_1 \geq 1$. In order to keep the form similar we shall want $\left[\frac{B_{n-1}}{n-1}+1\right]$ elements in some other class A_2 at the next stage. However the number of elements in A_2 is also given as $\left[\frac{\left[\frac{B_n}{n} + 1\right] - 1}{n-1} + 1\right]$. Hence we must have $B_{n-1} = \left[\frac{B_n}{n} + 1\right] - 1$ or $\left[\frac{B_n}{n} + 1\right] = B_{n-1} + 1$.

Now $B_n = \alpha_1 n + \beta_1$ so that $\left[\frac{B_n}{n} + 1\right] = \left[\frac{\alpha_1 n + \beta_1}{n} + 1\right]$ $= \left[\alpha_1 + \frac{\beta_1}{n} + 1\right] = \alpha_1 + 1$. Thus we must have $\alpha_1 = B_{n-1}$.

Also we take $\beta_1 = 1$, this being the smallest possible β_1 value under our assumptions. We choose β_1 as small as possible because we want to obtain as accurate an upper bound for $M(n)$ as is

possible. We now have $B_n = nB_{n-1} + 1$. We choose $B_0 = 1$ in order to keep B_n as small as possible. Thus we see that $B_n = T_n$. The only other possibility is the case $\beta_1 = 0$. Then $B_n = rn$ for some positive integral r. However we would have to have $r \geq (B_{n-1} + 1)$ which would give rise to a weaker upper bound for $M(n)$.

With this introduction let us now consider the estimation of the number $M^*(n)$, defined to be the smallest number of positive consecutive integers starting at 1 such that an arbitrary method of splitting the $M^*(n)$ numbers into n classes results in at least 1 solution of the equation $x + y = z$ in one or more classes <u>where we now stipulate $x \neq y$</u>. The argument leading to the determination of T_n^* (the upper bound for $M^*(n)$) proceeds as did the argument leading to the determination of the T_n. However if we have $\left[\frac{T_n^*}{n} + 1\right]$ elements in some class, say A_1, then we can only be certain of being able to form $\left(\left[\frac{T_n^*}{n} + 1\right] - 2\right)$ distinct differences which cannot lie in A_1 because it may be the case that one difference is of the form $a_r - a_1 = a_1$, in which case the difference does lie in A_1. We obtain an equation of the form $\left[\frac{T_{n-1}^*}{n-1} + 1\right] = \left[\frac{\left[\frac{T_n^*}{n} + 1\right] - 2}{n-1} + 1\right]$ which means that we must have $T_{n-1}^* = \left[\frac{T_n^*}{n} + 1\right] - 2$ or $\left[\frac{T_n^*}{n} + 1\right] = T_{n-1}^* + 2$. This equation leads to the recurrence relation

$$(1.7) \qquad T_n^* = \left(T_{n-1}^* + 1\right) n + 1 .$$

Once again we take $T_0^* = 1$. The first few values are

$T^*_1 = 3$, $T^*_2 = 9$, $T^*_3 = 31$, $T^*_4 = 129$ and $T^*_5 = 651$. For $n = 1$ and 2 it is found that $M^*(n) = T^*_n$. Walker [38], in connection with a problem proposed by Moser [16,17], states that $M^*(3) = 24$, $M^*(4) = 67$ and $M^*(5) = 197$ and further states that $2M^*(n) < M^*(n+1) < 3M^*(n)$ for $n \geq 2$. Again, Braun [5] states that $M^*(n) \geq \frac{3}{4}(3^n + 2n - 1)$. We now obtain a relation between T_n and T^*_n .

$$T^*_n = (T^*_{n-1} + 1)\,n + 1 = n\,T^*_{n-1} + n + 1$$

$$T^*_n = n\Big((T^*_{n-2} + 1)(n-1) + 1\Big) + n + 1 = n(n-1)\,T^*_{n-2} + n(n-1) + 2n + 1$$

$$T^*_n = n(n-1)\Big((T^*_{n-3} + 1)(n-2) + 1\Big) + n(n-1) + 2n + 1$$

$$T^*_n = n(n-1)(n-2)\,T^*_{n-3} + n(n-1)(n-2) + 2n(n-1) + 2n + 1$$

If we continue this process we evidently get

$$T^*_n = n(n-1)\ldots(n-(n-1))T^*_{n-(n)} + n(n-1)\ldots(n-(n-1)) + 2n(n-1)\ldots(n-(n-2)) + \ldots + 2n(n-1) + 2n + 1$$

$$T^*_n = n!\left(1 + \frac{1}{0!} + \frac{2}{1!} + \frac{2}{2!} + \ldots + \frac{2}{(n-2)!} + \frac{2}{(n-1)!} + \frac{1}{n!}\right)$$

Now $$2T_n = n!\left(2 + \frac{2}{1!} + \frac{2}{2!} + \ldots + \frac{2}{(n-1)!} + \frac{2}{n!}\right).$$

Hence

(1.8) $$T^*_n = 2T_n - 1 \quad .$$

The following remarks pertain to what we might call a 2 dimensional generalization of Schur's result. We try to make the 2 dimensional case as closely analogous to the 1 dimensional case as is possible. We consider those lattice points which have both co-ordinates positive. We construct an ordering relation

among these points as follows: Consider any 2 lattice points which we shall denote by $I\ (x_i, y_i)$ and $J\ (x_j, y_j)$. We say that I precedes J if $(x_i + y_i) < (x_j + y_j)$. Further, if $x_i + y_i = x_j + y_j$ we say that I precedes J if $y_i < y_j$. We shall say that $I + J = K$, where K is the lattice point having co-ordinates (x_k, y_k), if we have both $x_i + x_j = x_k$ and $y_i + y_j = y_k$. If vectors are drawn from the origin to the points in question we see that we have defined a vector addition. We further speak of the kth diagonal as the aggregate of points whose co-ordinates sum to $(k + 1)$. We associate the single positive integer $(k + 1)$ with the kth diagonal, $k \geq 1$. We now wish to estimate the number of lattice points required to force a solution of the form $I + J = K$ in at least one class when we separate the lattice points into n classes in an arbitrary manner.

Let us first consider the case where we separate the lattice points in such a way that all the diagonals remain intact. If Q_n refers to the smallest number of diagonals required to force a solution, we find that $Q_1 = 3$ and $Q_2 = 9$. In order that a solution exist, we must have I, J and K in one class where $(x_i + y_i) + (x_j + y_j) = (x_k + y_k)$. Furthermore, this condition is sufficient. We will always have the points $(a-1, 1)$, $(b-1, 1)$ and $(c-2, 2)$ at our disposal if $x_i + y_i = a$, $x_j + y_j = b$ and $x_k + y_k = c$ and so can force the equations $x_i + x_j = x_k$ and $y_i + y_j = y_k$ to hold. It therefore suffices to write down enough of the consecutive positive integers $2, 3, 4, \ldots$ to force a solution of the form $x + y = z$. Hence this part of the 2-dimensional problem reduces to a problem similar to that of Schur, except that we now start with the number 2. If we have r elements in some class and form the

(r-1) distinct "first differences" we may produce a difference, namely the number 1, which does not belong to the original set of integers. Hence we may produce only (r-2) differences which must belong to the other (n-1) classes. For this reason, the recurrence relation concerning the number of diagonals required to force a solution is exactly the same as for the T_n. If we denote by A_n this upper estimate for Q_n we shall have $A_0 = 1$ and $A_n = n(A_{n-1} + 1) + 1$. It is perhaps interesting that $Q_3 \geq 28$, as seen by the example shown, whereas $M_3 = 24$.

2	4	10
3	5	11
8	6	12
9	7	13
20	22	14
21	23	15
26	24	16
27	25	17
		18
		19

It is sufficient to take the first $\frac{A_n(A_n-1)}{2} + 2$ elements in order to force a solution.

If we now consider the general situation where diagonals need not remain intact we see that a solution is forced when we dispose of the element (T_n, T_n) by analogy with the one dimensional case. The number of elements required by the upper estimate in this case is $2\,T_n(T_n-1) + 1$.

We now discuss a more general theorem due to Rado[21], concerning problems of which Schur's problem is a special case.

An equation is said to be k-fold regular, k any positive integer, if it is possible, by taking a sufficient number of the consecutive positive integers 1, 2, ... and separating

them in an arbitrary manner into k classes, to force at least 1 solution of the equation in at least one of the classes. If an equation is k-fold regular for all possible values of k we speak of the equation as being regular.

In the present discussion we restrict ourselves to considering linear homogeneous equations with rational coefficients. We now consider some examples. Schur's theorem states, in terms of the present definitions, that the equation $x + y = z$ is regular. Brauer[2,3] showed that the equation $x + ay = z$ is regular. Consider now the equation $ax + by = 0$. If $a + b = 0$ then the equation is regular because a solution (in positive integers) is provided by taking $x = y = 1$. If $a + b \neq 0$ and a and b are of like sign then the equation cannot be solved when we restrict x and y to having positive integral values. Finally let us consider $a + b \neq 0$ but a and b of opposite sign. We write $y = -\frac{a}{b} x = cx$ where $c > 0$. We may assume, without loss of generality, that $c > 1$ (if $c < 1$ we interchange the rôles of x and y). The equation is 1-fold regular. If $a > 0, b < 0$ choose $x = -b$ and $y = a$ to obtain a solution. We now show, by means of a distribution of all positive integers, that $ax + by = 0$ is not 2-fold regular subject to our assumptions about a and b. We have just 2 classes, say A and B, and we want to split all the positive integers so that we cannot find x and $y = cx$ in the same class. Any positive integer m satisfies the relation $c^{\sigma} \leq m < c^{\sigma+1}$ for some $\sigma \geq 0$. We put into class A all those positive integers which are associated with an even value of σ. Then the numbers associated with an odd σ value appear in class B. However x and cx are

associated with 2 σ values, one of which is always even, the other being odd. Hence we can never find x and $y = cx$ in the same class. Thus $ax + by = 0$ is not 2-fold regular for $a + b \neq 0$, a and b of opposite sign. two

We now state and prove a theorem of Rado [21].

THEOREM 1.2:

If we are given the arbitrary but fixed positive integers a, b and c then there can always be found a positive integer N such that the equation $ax + by = cz$ is 2-fold regular where ~~we may find~~ $x, y, z \leq N$. It is always possible to find x_0, y_0, z_0 such that $ax_0 + by_0 = cz_0$. If $A = \max(x_0, y_0, z_0)$ and if m is the least common multiple of $\frac{a}{(a,b)}$ and $\frac{c}{(b,c)}$ then 18

$$(1.9) \qquad N = \max\left(mA, \ \frac{bm}{c}(A^2-1)(A-1) + \frac{bm}{c}A, \ \frac{bm}{a}A^2(A-1)\right)$$

((a,b) denotes the greatest common divisor of a and b).

As a simple example, consider the equation $2x + y = 5z$. Here we have $a = 2$, $b = 1$, $c = 5$ so that $(a,b) = (b,c) = 1$ and $m = 10$. The solution (x_0, y_0, z_0) of the equation which provides for the smallest value of A is $(2, 1, 1)$. Hence $A = 2$ so that $N = 20$. Hence we may conclude that if the numbers $1, 2, \ldots, 20$ are split into two classes in any arbitrary manner then we will have a solution of $2x + y = 5z$ in at least one of the classes. By considering various "small" solutions of the equation one finds that 15 is the smallest number of consecutive positive integers required to force a solution. Let us refer to the classes as B and C. If, by taking $x = \alpha$, $y = \beta$, $z = \gamma$ we obtain a solution of

$2x + y = 5z$ we shall use the notation (α, β, γ). $(2, 1, 1) \longrightarrow$ 1 and 2 cannot be in the same class. Let us put 1 in B, 2 in C. Then $(1, 3, 1) \longrightarrow 3$ is in C, $(4, 2, 2) \longrightarrow 4$ is in B, $(5, 5, 3) \longrightarrow 5$ is in B, $(2, 6, 2) \longrightarrow 6$ is in B, $(7, 6, 4) \longrightarrow 7$ is in C, $(8, 4, 4) \longrightarrow 8$ is in C, $(3, 9, 3) \longrightarrow 9$ is in B, $(5, 10, 4) \longrightarrow 10$ is in C, $(2, 11, 3) \longrightarrow 11$ is in B, $(4, 12, 4) \longrightarrow 12$ is in C, $(6, 13, 5) \longrightarrow 13$ is in C, $(14, 7, 7) \longrightarrow 14$ is in B. We are able to produce the array shown without forcing a solution but the solutions $(10, 15, 7)$ and $(5, 15, 5)$ make it impossible to continue.

B	C
1	2
4	3
5	7
6	8
9	10
11	12
14	13

We proceed to prove the theorem.

PROOF:

It will suffice to show that if we separate enough of the numbers 1, 2, ... in an arbitrary manner into two classes we shall force a solution of the equation $ax + by = cz$. We assume that there is a separation, which we denote by $\widetilde{S}$, of a certain number of the positive consecutive integers into two classes $\widetilde{R}_1$ and $\widetilde{R}_2$. We assume that there is no solution of $ax + by = cz$ in either $\widetilde{R}_1$ and $\widetilde{R}_2$ and proceed to obtain a contradiction. Let C be an arbitrary positive integer. Then the numbers C, 2C, 3C, ... AC cannot all lie in one class because as $A = \max(x_0, y_0, z_0)$, we would then have

x_0C, y_0C and z_0C in one class and a solution to the equation would be afforded by taking $x = x_0C$, $y = y_0C$ and $z = z_0C$ because $ax_0 + by_0 = cz_0$ implies $a(x_0C) + b(y_0C) = c(z_0C)$. Now put $x = m$. Consider the quantity $\frac{bx}{a}$. From the definition of m we must have $m = k_1 \frac{a}{(a,b)}$, for some positive integral k_1. Hence $\frac{bx}{a} = \frac{b}{(a,b)} k_1 \frac{a}{a}$. Also it must be the case that $(a,b) \mid b$. Hence $\frac{bx}{a}$ is integral. Similarly $\frac{bx}{c}$ is integral. We can put x in $\tilde{R}_1$ without loss of generality and so we do this. Then we know that not all the numbers $m, 2m, \dots Am$ can be in $\tilde{R}_1$ from the first argument. Let $y = \ell m$, where $2 \le \ell \le A$, be the first of these numbers which lies in $\tilde{R}_2$. We form the number $\frac{b}{a}(y-x) = \frac{b}{a}(\ell-1)m$ which is seen to be a positive integer and then consider $z = n\frac{b}{a}(y-x) = n\frac{b}{a}(\ell-1)m$ where n is an arbitrary positive integer. We assume that z is in $\tilde{R}_2$ and draw some conclusions. The number

$$(1.10) \qquad \frac{a}{c}z + \frac{b}{c}y = \frac{a}{c}n\frac{b}{a}(\ell-1)m + \frac{b}{c}\ell m$$

$$= \frac{bm}{c}(n\ell - n + \ell) = \frac{bm}{c}(n(\ell-1)+\ell)$$

is a positive integer. If this number is in $\tilde{R}_2$ then $au + bv = cw$ where $u = z$, $v = y$ and $w = \frac{a}{c}z + \frac{b}{c}y$. Hence $\frac{a}{c}z + \frac{b}{c}y$ must be in $\tilde{R}_1$. The number

$$(1.11) \qquad \frac{c}{a}\left(\frac{a}{c}z + \frac{b}{c}y\right) - \frac{b}{a}x = z + \frac{b}{a}(y-x) = (n+1)\frac{b}{a}(y-x) = (n+1)\frac{b}{a}(\ell-1)m$$

is a positive integer which must be in $\tilde{R}_2$. If not, we shall have $au + bv = cw$ in $\tilde{R}_1$ where $u = \frac{c}{a}\left(\frac{a}{c}z + \frac{b}{c}y\right) - \frac{b}{a}x$, $v = x$ and $w = \frac{a}{c}z + \frac{b}{c}y$. w has just been shown to be in $\tilde{R}_1$. The assumption that $z = n\frac{b}{a}(\ell-1)m$ was in $\tilde{R}_2$ leads us to conclude

$(n+1)\frac{b}{a}(\ell-1)m$ is also in $\tilde{R}_2$. To effect the proof we now take $C = \frac{b}{a}(y-x)$. Then $z = nC$ and assuming that nC is in $\tilde{R}_2$ forces $(n+1)C$ to be in $\tilde{R}_2$ also. Now we know that $C, 2C, \ldots AC$ cannot all lie in $\tilde{R}_1$. Hence there must exist some positive integer $n_o \leq A$ such that n_oC is in $\tilde{R}_2$. By our inductive step, n_oC in $\tilde{R}_2$ implies $(n_o+1)C$ in $\tilde{R}_2$. If we take $n = n_o, n_o+1, \ldots 2n_o, \ldots 3n_o, \ldots (An_o-1)$ successively we find that the numbers $n_oC, (n_o+1)C, \ldots n_o2C, \ldots 3Cn_o, \ldots ACn_o$ all lie in $\tilde{R}_2$. Hence we shall have $x_o(n_oC)$, $y_o(n_oC)$ and $z_o(n_oC)$ all in $\tilde{R}_2$ and thus we have forced a solution of the equation in the class $\tilde{R}_2$. The larger numbers involved in the construction give us an estimate of the number of positive integers required. We have used the numbers $x = m$, $y = m$, $nC = n\frac{b}{a}(\ell-1)m$, $\frac{bm}{c}\left(n(\ell-1)+\ell\right)$ and $(n+1)C = (n+1)\frac{b}{a}(\ell-1)m$. We maximize these quantities, obtaining $m, Am, \frac{b}{a}(A^2-1)(A-1)m, \frac{bm}{c}(A^2-1)(A-1) + \frac{bm}{c}A$, and $\frac{b}{a}A^2(A-1)m$.

A sufficiently large number of positive integers will be considered if we choose the maximum available among these quantities. We denote this number by N. Then

$$N = \max.\left(m\,A,\ \frac{bm}{c}(A^2-1)(A-1)+\frac{bm}{c}A,\ \frac{b}{a}A^2(A-1)m\right)$$

Hence the theorem is proved.

The results noted may be summarized by saying that the equation $\sum_{\nu=1}^{n} a_\nu x_\nu = 0$, where the coefficients a_ν are rational, is 2-fold regular if and only if at least one of the following conditions holds:

(i) $\sum_{\nu=1}^{n} a_\nu = 0$

(ii) At least three of the coefficients are nonzero and the a_ν are not all of the same sign.

PROOF:

If neither of (i), (ii) holds then $\sum_{\nu=1}^{n} a_\nu \neq 0$ and not more than two coefficients are nonzero. We allow these coefficients any sign. $\sum_{\nu=1}^{n} a_\nu \neq 0$ implies the existence of at least one nonzero coefficient. We have just two possibilities.

(a) $a_1 x_1 = 0 \qquad a_1 \neq 0$

(b) $a_1 x_1 + a_2 x_2 = 0 \qquad a_1 + a_2 \neq 0$.

In (a), $x_1 = 0$ is the only way of having the equation hold and the variables are restricted to positive integral values. Hence (a) is not k-regular for any k whatsoever. In particular it is not 2-fold regular. If a_1 and a_2 are of like sign in (b) then the conclusions of (a) with respect to regularity are applicable. If a_1 and a_2 are of opposite sign we do not have 2-fold regularity by the example done previously. If (i) holds then the equation is regular because it suffices to take $x_\nu = 1$ for $1 \leq \nu \leq n$. If (ii) is satisfied we may always put the equation in the form $\sum_{\rho=1}^{r} b_\rho y_\rho = \sum_{\sigma=1}^{s} c_\sigma z_\sigma$ where b_ρ, c_σ are positive integers. Take $y_2 = y_3 = \ldots = y_r$ and $z_1 = z_2 = \ldots = z_s$. We then obtain an equation of the form

$$b_1 y_1 + \left(\sum_{\rho=1}^{r} b_\rho \right) y_2 = \left(\sum_{\sigma=1}^{s} c_\sigma \right) z_1$$

which is 2-fold regular being of the form of Theorem 1.2.

CHAPTER II

Introduction. In this chapter we first consider two results concerning a theorem of van der Waerden[33-36]. These results are lower bounds for the van der Waerden function $W(k,\ell)$. The second part of the chapter is a discussion of a number of results dealing with "progression-free" sets.

We begin by stating a theorem of van der Waerden[33-36].

THEOREM 2.1:

Given any two arbitrary positive integers k and ℓ, there exists a positive integer m such that, if any m consecutive integers are separated into not more than k classes in any manner whatsoever, then at least one class will contain at least $(\ell + 1)$ numbers which form an arithmetic progression.

The proof of this theorem will not be given here. Proofs appearing in the literature include those of Lukomskaya[14], Witt[39], and Grünwald in a paper of Rado[22].

We shall denote by $W = W(k,\ell)$ (van der Waerden's function) the least number m possessing the property mentioned above. The existing proofs of van der Waerden's theorem lead to extremely large upper estimates of W. We concern ourselves only with lower estimates for W.

Erdös and Rado[11] have proved the following: let k and ℓ be integers not less than 2, and let m_0 be the largest integer such that $m_0{}^2 \leq 2\ell k^{\ell}$. Then there exists a distribution of the set $\tilde{S}_0 = \{1, 2, \ldots, m_0\}$ into not more than k classes such that no class contains $(\ell + 1)$ elements in arithmetic progression. That is,

(2.1) $\quad W(k,\ell) > (2\ell k^{\ell})^{\frac{1}{2}}$.

PROOF:

Since $W(1,\ell) = \ell + 1$ and $W(k,1) = k + 1$ we are just excluding these trivial cases by having $k, \ell \geq 2$. We assume that, given any distribution of the set $\tilde{S} = \{1, 2, \ldots, m\}$ into not more than k classes, there exist positive numbers c and d such that $c, c + d, \ldots, c + \ell d$ are all elements of a single class. We show that $m^2 > 2\ell k^{\ell}$. We have $m \geq \ell + 1$ because otherwise it would certainly be impossible to have an arithmetic progression containing $(\ell + 1)$ elements. The largest element of the progression is to be of the form $(c + \ell d)$. Clearly, d is confined to the range $1 \leq d \leq \left[\frac{m-1}{\ell}\right]$. Given any particular d value in the range, the number of arithmetic progressions of $(\ell + 1)$ terms with common difference d and elements in $\tilde{S}$ is $(m - \ell d)$. Hence the total number of such progressions, for varying d, is

$$(2.2) \qquad M = \sum_{d=1}^{\left[\frac{m-1}{\ell}\right]} (m - \ell d) \leq \frac{m-1}{\ell}\, m - \frac{\ell}{2}\, \frac{m-1}{\ell}\left(\frac{m-1}{\ell} + 1\right)$$

$$M \leq \frac{m-1}{2\ell}\,(2m - m + 1 - \ell) < \frac{m^2 - 1}{2\ell} < \frac{m^2}{2\ell} .$$

The total number of ways of splitting the set $\tilde{S}$ into not more than k classes is k^m. We now insist upon having an arithmetic progression of $(\ell + 1)$ elements. As mentioned above, we have M choices for such a progression. The remaining $m - (\ell + 1)$ elements may occur in any class and hence we have a factor of $k^{m-(\ell+1)}$. Finally, we have k choices regarding the class in which the progression is to be

found. We now must have, because of our initial assumption,

$$(2.3) \qquad k\,M\,k^{m-(\ell+1)} \geq k^m$$

Thus $k^{\ell} \leq M < \dfrac{m^2}{2\ell}$ so that $m^2 > 2\ell k^{\ell}$, as required.

We now discuss a result of Moser [15], who proved that, for a suitable constant c_6,

$$(2.4) \qquad W(k,\ell) > W(k,2) > k^{c_6 \log k}$$

PROOF:

Consider the numbers $1, 2, \ldots, 2^{2N^2}-1$. Any integer x in this range, when written in the base 2^N, is of the form

$$(2.5) \qquad x = a_{2N}(2^N)^{2N-1} + a_{2N-1}(2^N)^{2N-2} + \ldots + a_2(2^N)^1 + a_1(2^N)^0 ,$$

where the coefficients a_r, $(1 \leq r \leq 2N)$, must satisfy $0 \leq a_r \leq (2^N-1)$. For each x we define a "signature", $s(x)$, in the following way: let $\epsilon_r \equiv a_r \pmod 2$, then

$$(2.6) \qquad s(x) = \epsilon_{2N}(2^N)^{2N-1} + \epsilon_{2N-1}(2^N)^{2N-2} + \ldots + \epsilon_2(2^N)^1 + \epsilon_1(2^N)^0 .$$

We also define, for each x, a "modulus", $m(x)$, given by

$$(2.7) \qquad m(x) = \sum_{r=1}^{2N} a_r^2$$

We proceed to separate the $(2^{2N^2}-1)$ numbers being considered into classes, putting two numbers in the same class if and only if they have the same signature and the same modulus. We proceed to prove that no three distinct elements of a single class can be in arithmetic progression. We assume that there exist distinct elements

$$B = \sum_{r=1}^{2N} b_r (2^N)^{r-1} , \qquad C = \sum_{r=1}^{2N} c_r (2^N)^{r-1}$$

and D in the same class such that $B + C = 2D$. Then we have

$$D = \sum_{r=1}^{2N} \frac{b_r + c_r}{2} (2^N)^{r-1} , \qquad \frac{b_r + c_r}{2}$$

being integral for all r since the signatures of B and C are equal. By assumption we must have

$$(2.8) \qquad m(D) = m(B) = m(C)$$

$$\sum_{r=1}^{2N} \left(\frac{b_r + c_r}{2}\right)^2 = \sum_{r=1}^{2N} (b_r)^2 = \sum_{r=1}^{2N} (c_r)^2$$

Now

$$\sum_{r=1}^{2N} \left(\frac{b_r + c_r}{2}\right)^2 = \frac{1}{2} \sum_{r=1}^{2N} b_r^2 + \frac{1}{2} \sum_{r=1}^{2N} b_r c_r$$

$$\sum_{r=1}^{2N} \left(\frac{b_r + c_r}{2}\right)^2 = \frac{1}{2} \sum_{r=1}^{2N} c_r^2 + \frac{1}{2} \sum_{r=1}^{2N} b_r c_r .$$

Thus we must have

$$(2.9) \qquad \sum_{r=1}^{2N} b_r c_r = \sum_{r=1}^{2N} b_r^2$$

and

$$(2.10) \qquad \sum_{r=1}^{2N} b_r c_r = \sum_{r=1}^{2N} c_r^2 .$$

These two equations require that $\sum_{r=1}^{2N} (b_r - c_r)^2 = 0$ which, in turn, requires that $b_r = c_r$ for all r. Hence for (2.8) to hold we must have $B = C$. Thus we have arrived at the required contradiction. We proceed to determine the number of classes constructed. The number of signatures is 2^{2N}

and the number of possible moduli is less than $2N \cdot 2^{2N}$. Hence the number of classes is less than $2N \cdot 2^{4N} \leq 2^{5N}$.

Given $k = 2^5 k'$, N is uniquely determined by

$$(2.11) \qquad 2^{5(N-1)} < k' \leq 2^{5N}.$$

Since we are able to put 2^{2N^2} numbers into 2^{5N} classes we have $W(2^{5N}, 2) > 2^{2N^2}$. However, $2^{2N^2} = 2^{5N \cdot c_1 N} > (k')^{c_2 \log_2 k'} = (c_3 k)^{c_4 \log k + c_3} > k^{c_6 \log k}$ where $c_1, c_2, \ldots, c_6$ are suitable constants. Also, since $k > 2^{5N}$, we have $W(k, 2) > W(2^{5N}, 2)$. Finally, we may write $W(k, 2) > k^{c_6 \log k}$. A theorem of Roth [23-25] which we discuss later in the chapter makes it possible to show that $W(k, 2) < e^{e^{c_7 k}}$ for a suitable constant c_7.

It is interesting to compare the two lower bounds discussed, (2.1) and (2.4). The former is relatively insensitive to changes in k whereas the latter is totally insensitive to changes in ℓ. Thus, depending on the relative size of k and ℓ, we choose between (2.1) and (2.4).

We define a "progression-free" or " non-averaging" set to be a set of non-negative integers S: $o \leq s_1 < s_2 < \ldots$ which does not contain the average of any two of its elements, i.e. $s_i + s_j \neq 2s_k$ $(i \neq j)$. Thus no three elements of such a set form an arithmetic progression. We denote by $\nu(N)$ the number of elements of a "progression-free" set which do not exceed N.

We proceed to discuss various lower and upper estimates for the function $\nu(N)$. Salem and Spencer [26,27] proved that, for every $\epsilon > 0$ and sufficiently large N,

$$(2.12) \qquad \nu(N) > N^{1 - \frac{\log 2 + \epsilon}{\log \log N}}.$$

We consider a refinement due to Behrend [1], who proved that for every $\epsilon > 0$ and sufficiently large N,

$$(2.13) \qquad \nu(N) > N^{1 - \frac{2\sqrt{2 \log 2} + \epsilon}{\sqrt{\log N}}} .$$

Taking $n \geq 2$, $d \geq 2$ we consider all numbers of the form

$$(2.14) \qquad B = \sum_{i=1}^{n} b_i (2d-1)^{i-1}$$

where the coefficients b_i must satisfy $0 \leq b_i \leq (d-1)$, $(1 \leq i \leq n)$. We associate with each such number a "norm", defined as $(\text{norm } B)^2 = k = \sum_{i=1}^{n} b_i^2$. We separate the numbers of the above type into sets, putting two numbers in the same set if they have the same "norm". We denote a set with "norm" equal to $\sqrt{k}$ by $S_k(n,d)$. We now prove that any such set $S_k(n,d)$, $(0 \leq k \leq n(d-1)^2)$, is a "progression-free" set. We assume that there exist three elements, say A, A' and A'' in $S_k(n,d)$ such that $A + A' = 2A''$. We show that these conditions imply $A = A' = A''$. Since $A + A' = 2A''$ we must have norm $(A + A') =$ norm $(2A'')$. In general, norm $B = \sqrt{b_1^2 + b_2^2 + \ldots + b_n^2}$ so that norm $2B = \sqrt{(2b_1)^2 + (2b_2)^2 + \ldots + (2b_n)^2} = 2$ norm B. Hence norm $(A + A') = 2$ norm $A'' = 2\sqrt{k}$ because A'' is an element of $S_k(n,d)$. However, $2\sqrt{k} =$ norm A + norm A' so that $A + A' = 2A''$ implies that we must have

$$(2.15) \qquad \text{norm } (A + A') = \text{norm } A + \text{norm } A' .$$

Employing the type of argument used in the proof of $\nu(k, \ell) > k^{c_6 \log k}$ we find that the triangular inequality

$$(2.16) \qquad \text{norm } (A + A') \leq \text{norm } A + \text{norm } A'$$

holds generally and that equality holds only when the coefficients of A and A' are proportional. However, since norm A = norm A', we must have $A = A'$.

The range of k shows that we have produced $(n(d-1)^2 + 1)$ progression-free sets. The number of non-negative integers involved in these sets is d^n. Hence there exist at least $\dfrac{d^n}{n(d-1)^2 + 1}$ elements in at least one of these "progression-free" sets. Since $(n(d-1)^2 + 1)$ is less than $n\,d^2$ for the ranges of n and d under discussion, we must have more than $\dfrac{d^{n-2}}{n}$ elements in some $S_k(n,d)$. The largest positive integer is

$$(d-1)\,1 + (2d-1)^1 + \ldots + (2d-1)^{n-1} = \frac{(2d-1)^n - 1}{2} < (2d-1)^n .$$

We have thus shown that $\nu((2d-1)^n) > \dfrac{d^{n-2}}{n}$. Let N be given. Since n and d are at our disposal, we take $n = \left[\sqrt{\dfrac{2\log N}{\log 2}}\right]$, d such that $(2d-1)^n \leq N < (2d+1)^n$. Now $d > \left(\dfrac{N^{\frac{1}{n}} - 1}{2}\right)$ which enables us to write

$$(2.17) \qquad \nu(N) \geq \nu((2d-1)^n) > \frac{d^{n-2}}{n} > \frac{(N^{\frac{1}{n}} - 1)^{n-2}}{n \cdot 2^{n-2}} = \frac{N^{1-\frac{2}{n}}(1 - N^{-\frac{1}{n}})^{n-2}}{n \cdot 2^{n-2}} .$$

Consider the quantity $(1 - \dfrac{1}{N^{\frac{1}{n}}})^{n-2}$. For sufficiently large N we have, expanding using the binomial theorem,

$$(2.18) \qquad \left(1 - \frac{1}{N^{\frac{1}{n}}}\right)^{n-2} = 1 + (n-2)\left(\frac{-1}{N^{\frac{1}{n}}}\right) + \frac{(n-2)(n-3)}{2!}\left(\frac{-1}{N^{\frac{1}{n}}}\right)^2 + \ldots + 0 .$$

Since the terms alternate in sign and decrease in magnitude we may write $\left(1 - \dfrac{1}{N^{\frac{1}{n}}}\right)^{n-2} > 1 - \dfrac{(n-2)}{N^{\frac{1}{n}}}$. Since $n = \left[\sqrt{\dfrac{2\log N}{\log 2}}\right]$, $N^{\frac{1}{n}}$ acts as 2^n for sufficiently large N. Hence $\left(1 - \dfrac{1}{N^{\frac{1}{n}}}\right)^{n-2} > \dfrac{1}{2}$

for such N. Thus $\nu(N) > \dfrac{N^{1-\frac{2}{n}}}{n \cdot 2^{n-1}}$ for sufficiently large N.

Since $\log(n \cdot 2^{n-1}) = \log n + (n-1)\log 2$ we write

$$n \cdot 2^{n-1} = N^{\frac{1}{\log N}(\log n + (n-1)\log 2)} .$$ Hence

$$\nu(N) > N^{1 - \frac{2}{n} - \frac{\log n}{\log N} - (n-1)\frac{\log 2}{\log N}} \tag{2.19}$$.

From (2.19) we see that for any $\epsilon > 0$ and sufficiently large N we have

$$\nu(N) > N^{1 - \frac{2\sqrt{2 \log 2} + \epsilon}{\sqrt{\log N}}} \tag{2.20}$$.

Moser [18] has given a constructive definition of a "progression-free" sequence for which

$$\nu(N) > N^{1 - \frac{c}{\sqrt{\log N}}} \tag{2.21}$$

for c a fixed positive constant.

Upper estimates have been given by Erdös and Turán [12], who found, for every $\epsilon > 0$ and N sufficiently large, that $\nu(N) < \left(\frac{3}{8} + \epsilon\right) N$, and by Moser [18], who proved that $\nu(N) < \frac{4}{11} N + 5$. Finally, Roth [23-25] proved that any "progression-free" set must have zero asymptotic density. More precisely, if $u_1, u_2, \ldots u_{\nu(x)}$ are distinct positive integers not exceeding x and if the equation $u_i + u_j = 2u_h$ has no solution with $i \neq j$, then $\nu(x) = O\left(\frac{x}{\log\log x}\right)$. Using this result, Varnavides [37] has proved the following:

THEOREM 2.2:

Let δ be any number with $0 < \delta < 1$ and let $a_1, a_2, \ldots a_m$ be distinct positive integers not exceeding x. Suppose that $x > x_0(\delta)$, $m > \delta x$, where $x_0(\delta)$ depends only on δ. Then the number of solutions of $a_i + a_j = 2a_h$, $i \neq j$ is at least $C(\delta)\, x \log x$, where $C(\delta)$ is a positive number depending only on δ.

PROOF:

It follows from Roth's theorem that in any sequence of positive asymptotic density there must occur at least one solution of $u_i + u_j = 2u_h$ with $i \neq j$. We restate Roth's result in a convenient form: Let δ' be any number satisfying $0 < \delta' < 1$, and let $b_1, b_2, \ldots b_n$ be distinct positive integers less than x. Suppose that $x > x_1(\delta')$, $n > \delta' x$, where $x_1(\delta')$ is a certain number which depends only on δ'. Then there exists at least one solution of $b_i + b_j = 2b_h$ with $i \neq j$. We now choose an integer $k = k(\delta)$, only such that $k > x_1(\frac{\delta}{2})$. Then the result above, with k replacing x, $\frac{\delta}{2}$ replacing δ', will be applicable to any set of n integers, where $n > \delta' x = \frac{\delta k}{2}$. We define a number r so that $k^r < \frac{x}{2}$. Any integer t not exceeding x has a unique representation of the form

$$(2.22) \qquad t = c_0 + c_1 k + \ldots + c_{r-1} k^{r-1} + d\, k^r$$

where $0 \leq c_i \leq (k-1)$, $(0 \leq i \leq r-1)$ and where $0 \leq d \leq k^{-r} x$. Consider a number ν which may assume any one of the values $0, 1, \ldots (r-1)$. For any particular value of ν, we separate

the integers not exceeding x into classes by putting in the same class those integers for which d and all of $c_0, c_1, \dots c_{r-1}$, except c_ν, have the same values. The total number of classes will thus be $k^{r-1}\left[k^{-r}x + 1\right]$. It is clear that no class contains more than k elements. We define a "good" class to be a class which contains more than $\frac{\delta k}{2}$ numbers of the given set of positive integers $a_1, a_2, \dots, a_m$. If a class is not "good", it is said to be "bad". Even if all the classes were "bad" the total number of elements of the set $a_1, a_2, \dots, a_m$ could not exceed

$$(2.23) \qquad k^{r-1}\left[k^{-r}x + 1\right]\frac{\delta k}{2} \quad \leq \quad \frac{\delta}{2}\,(x + k^r)\,.$$

If we denote by N the number of "good" classes, the number of a's contained by these classes cannot exceed Nk. Hence we must have

$$(2.24) \qquad \frac{\delta}{2}\,(x + k^r) + Nk > m > \delta x$$

which implies, using the fact that $k^r < \frac{x}{2}$, that $N > \frac{\delta}{4}\, x\, k^{-1}$. If, in any "good" class, we vary c_ν, $(0 \leq c_\nu \leq k-1)$, then we must produce more than $\frac{\delta k}{2}$ elements of the set $a_1, a_2, \dots a_m$ because of the definition of good class. The restatement of Roth's result is applicable to the c_ν values so that there must be three of these values which are in arithmetic progression. It is clear that the corresponding a's will also be in arithmetic progression. If we denote by $c_\nu^{(i)}$ the c_ν value corresponding to a_i we must have

$$(2.25) \qquad a_i - a_j = \left(c_\nu^{(i)} - c_\nu^{(j)} \right) k^\nu$$

and since $1 \leq \left| c_\nu^{(i)} - c_\nu^{(j)} \right| \leq (k-1)$

$$(2.26) \qquad k^\nu \leq \left| a_i - a_j \right| < k^{\nu+1} .$$

Hence for each ν we must have at least N solutions of $a_i + a_j = 2a_h$, $i \neq j$ which satisfy (2.26). From (2.26) we see that as ν is varied the solutions obtained will all be distinct. Hence the total number of solutions is at least

$$(2.27) \qquad r N > \frac{\delta}{4} x k^{-1} r .$$

From the relation $k^r < \frac{x}{2}$ together with (2.24) we may conclude that r is proportional to $\log x$ for large x. Hence (2.27) is of the form required by the statement of the theorem.

CHAPTER III

Introduction. In this chapter we begin by considering the following problem: let the first $2n$ consecutive positive integer $1, 2, \ldots, 2n$ be separated into two disjoint classes $\tilde{A}$ and $\tilde{B}$, each class containing n elements. The separation of these numbers is to be arbitrary in all other respects. We write $\tilde{A} : \{a_i\}$, a_i being any element of $\tilde{A}$, $(1 \leq i \leq n)$. We also order the n elements of the class $\tilde{A}$, obtaining $1 \leq a_1 < a_2 < \ldots < a_n \leq 2n$. The class $\tilde{B}$ is dealt with in a similar way, so that we write $\tilde{B} : \{b_j\}$, $(1 \leq j \leq n)$, $1 \leq b_1 < b_2 < \ldots < b_n \leq 2n$. Using the classes $\tilde{A}$ and $\tilde{B}$ we form the "difference set" $(\tilde{A}-\tilde{B})$: $\{a_i - b_j\}$ where, as above, we have $(1 \leq i \leq n)$, $(1 \leq j \leq n)$. For k in the range $|k| \leq (2n-1)$ we want to obtain estimates for the maximum number of solutions of an equation of the form $a_i - b_j = k$.

The second problem is concerned with a set of distinct positive integers, none of which exceeds n. We order the elements of such a set, obtaining $1 \leq a_1 < a_2 < \ldots < a_k \leq n$. The number k is to be maximal. We insist that all sums of the form $a_{i_1} + a_{i_2} + \ldots + a_{i_r}$, $(0 \leq r \leq k)$, be distinct. We want to determine, subject to the conditions mentioned, how large $k = k(n)$ can be.

The first problem was originally stated in terms of the $4n$ numbers $1, 2, \ldots, 4n$. Erdös [8,9] conjectured that there exists at least one integer r, $|r| \leq (4n-1)$, such that the equation $a_\ell - b_m = r$, $(1 \leq \ell \leq 2n)$, $(1 \leq m \leq 2n)$, has at least n solutions. If we choose $a_1 = n+1$, $a_2 = n+2$, $\ldots$, $a_{2n} = 3n$ we see that the value n, if true, would be the best possible result. However the conjecture has been shown to be false and we shall revert to the form of the problem mentioned in the introduction.

Let us define $M_k = \sum_{a_i - b_j = k} 1$ i.e. M_k is the number of solutions of the equation $a_i - b_j = k$. We also denote by ξ any separation of the $2n$ numbers into two classes $\tilde{A}$ and $\tilde{B}$. Finally we define

$$(3.1) \qquad M = \min_{\xi} \left(\max_k M_k \right) .$$

Thus $M = M(n)$ only.

We discuss certain lower estimates which have been obtained for $M(n)$. In the difference class $(\tilde{A}-\tilde{B})$ we have n^2 elements which are non-zero and which all occur in the range $|a_i - b_j| \leq (2n-1)$. Since we have n^2 elements occurring in a range of less than $4n$ it must be the case that $M_k > n/4$ for some k. Hence we conclude that $M(n) > \frac{n}{4}$. Scherk [9] has improved this estimate by showing that $M(n) > \frac{n}{2}(2-\sqrt{2}) > 0.29n$. We now consider a further improvement due to Moser [15]. We define

$$A = \sum_{i=1}^{n} a_i , \qquad B = \sum_{j=1}^{n} b_j \qquad \text{and} \qquad P = \sum_{i,j} (a_i - b_j) .$$

It is clear that we may write

$$(3.2) \qquad P = \sum_k k M_k = \sum_{i,j} (a_i - b_j) = n(A-B) .$$

The approach used here is essentially statistical in nature. The n^2 elements of the difference set $(\tilde{A}-\tilde{B})$ constitute a finite population. If we were to plot M_k against k, and assumed an optimal separation of the $2n$ numbers, then M would be the mode of the resulting distribution. Our aim here is to show that M is "large", regardless of the manner in which $1, 2, \ldots, 2n$ are separated. If the distribution were rectangular then the mode would have a minimum value, but this value must exceed $\frac{n}{4}$. This result is just another way of stating a remark made above. If we can show that the actual distribution must differ considerably from a rectangular distribution then we will be able to conclude that $M(n)$ is fairly "large". We now define

$$(3.3) \qquad Q = \sum_{i,j} (a_i - b_j)^2 = n \sum_{i=1}^{n} a_i^2 + n \sum_{j=1}^{n} b_j^2 - 2 \sum_{i,j} a_i b_j \ .$$

We have

$$\sum_{i,j} a_i b_j = AB \quad \text{and} \quad \sum_{i=1}^{n} a_i^2 + \sum_{j=1}^{n} b_j^2 = 1^2 + 2^2 + \ldots + (2n)^2$$

so that

$$(3.4) \qquad Q = \frac{n\,(2n)(2n+1)(4n+1)}{6} - 2AB \qquad .$$

We also define

$$(3.5) \qquad R = \sum_{i,j} (a_i - b_j - \frac{P}{n^2})^2 = Q-(A-B)^2 = \frac{n\,(2n)(2n+1)(4n+1)}{6} - (A^2+B^2)$$

$$\text{Since} \qquad A^2 + B^2 = \frac{(A+B)^2}{2} + \frac{(A-B)^2}{2} = \frac{(2n)^2\ (2n+1)^2}{8} - \frac{(A-B)^2}{2}$$

we obtain

$$(3.6) \qquad R = \frac{n^2(4n^2-1)}{6} - \frac{(A-B)^2}{2} \leq \frac{n^2(4n^2-1)}{6} .$$

Having obtained an upper bound for R, we now want to obtain a lower bound. We notice that, while $\frac{A-B}{n}$ need not be integral, the values of the expression $(a_i - b_j - \frac{A-B}{n})$ differ by integers. We assume that the numbers $1, 2, \ldots, 2n$ have been separated so that no value of k is produced more than M times. Since $(a_i - b_j - \frac{A-B}{n})^2 \geq 0$ we may conclude that

$$(3.7) \qquad R \geq M\,(0^2 + 1^2 + (-1)^2 + \ldots + (u-1)^2 + (1-u)^2 + u^2 + w^2)$$

where $w = 0$ when $\left[\frac{n^2}{M}\right] = 2u$, $w = -u$ when $\left[\frac{n^2}{M}\right] = 2u+1$. We consider these two cases separately.

<u>Case I</u> $\left[\frac{n^2}{M}\right] = 2u+1$ so that $w = -u$. In this case,

$$(3.8) \qquad R \geq 2M \frac{u(u+1)(2u+1)}{6} = \frac{M\,2u(2u+1)(2u+2)}{12} .$$

Since $2u+1 \leq \frac{n^2}{M} < 2(u+1)$ we must have

$$(3.9) \qquad R > \frac{n^2}{12}\left(\frac{n^2}{M} - 2\right)\left(\frac{n^2}{M} - 1\right) .$$

<u>Case II</u> $\left[\frac{n^2}{M}\right] = 2u$ so that $w = 0$. In this case,

$$(3.10) \qquad R \geq 2M\left(\frac{(u-1)\,u\,(2u-1)}{6} + \frac{u^2}{2}\right) = \frac{M}{3}\,u(2u^2+1).$$

Since $2u \leq \frac{n^2}{M} < 2u+1$ we can make the statement (3.9) for this case also.

Hence we have shown that

$$(3.11) \qquad \frac{n^2\,(4n^2-1)}{6} \geq R > \frac{n^2}{12}\left(\frac{n^2}{M}-2\right)\left(\frac{n^2}{M}-1\right) \quad .$$

Assuming the form $M = \alpha\, n$ we can conclude, using (3.11) that $\alpha \geq \dfrac{1}{2\sqrt{2}}$.

Hence $\quad M(n) \geq \dfrac{n}{2\sqrt{2}} > 0.35n$.

By combining this argument with that of Scherk, Moser [15] has shown that $M(n) > 0.356n$.

As noted previously, the conjecture of Erdös [8,9] was that $M(n) \geq \dfrac{n}{2}$. Erdős himself has shown that the conjecture was false and has proved that $M(n) \leq \dfrac{4}{9}n$. Motzkin, Ralston and Selfridge [19] studied this problem, using the digital computer "SWAC". They have shown that $M(n) > 0.4n$ is false by means of the following example, in which $n = 15$, $M(n) = 6$:

A: 1, 2, 3, 4, 6, 7, 12, 14, 21, 24, 25, 27, 28, 29, 30

B: 5, 8, 9, 10, 11, 13, 15, 16, 17, 18, 19, 20, 22, 23, 26.

Let us now consider a set of distinct positive integers $1 \leq a_1 < a_2 < \ldots < a_k \leq n$. We insist that the 2^k numbers of the form $a_{i_1} + a_{i_2} + \ldots + a_{i_r}$, $(0 \leq r \leq k)$, be distinct. ? $2^k - 1$ Suppose further that k is as large as possible. We want to obtain upper and lower estimates of $k = k(n)$.

Given any arbitrary n there exists a unique non-negative integer t such that $2^t \leq n < 2^{t+1}$. If we let $a_\nu = 2^\nu$, $(0 \leq \nu \leq t)$, we obtain $(t+1) = [\log_2 n] + 1$ distinct positive integers not exceeding n. Since the binary representation of an integer is unique it is clear that the 2^k subsets are

distinct. Thus we have

(3.12) $\quad k(n) \geq [\log_2 n] + 1$.

The sum of the largest subset is $a_1 + a_2 + \ldots + a_k < k\,n$. Since the subset sums are all non-negative and distinct we must have $2^k \leq kn$. Hence $k \leq \log_2 k + \log_2 n$. Certainly $k \leq 2 \log_2 n$ so that

(3.13) $\quad k \leq \log_2 n + \log_2 \log_2 n + 1$.

We now discuss a result of Erdös and Moser [9] who have shown that

(3.14) $\quad k < \log_2 n + \dfrac{\log_2 \log_2 n}{2} + \dfrac{5}{2}$.

We denote the sum of the elements of the ith subset by s_i, $1 \leq i \leq 2^k$. Let us define $A = \sum_{j=1}^{k} a_j$. The arithmetic mean mean of all the subset sums is $\dfrac{\sum_{i=1}^{2^k} s_i}{2^k}$. In order to evaluate this expression, we pair off each subset with its complement (with respect to the set $a_1, a_2, \ldots, a_k$). The sum of the elements in such a pair is clearly A. Since we have 2^{k-1} such pairs we must have

(3.15) $\quad \dfrac{\sum_{i=1}^{2^k} s_i}{2^k} = \dfrac{A}{2}$.

Let us now obtain an estimate for the quantity $\sum_{1 \leq i \leq 2^k} (s_i - \frac{A}{2})^2$.

We have

$$\sum_{1\le i\le 2^k} (s_i - \frac{A}{2})^2 = \sum_{1\le i\le 2^k} \frac{(2s_i-(a_1+a_2+\ldots+a_k))^2}{4} = \frac{1}{4}\sum(\pm a_1 \pm a_2 \ldots \pm a_k)^2$$

where the last sum extends over the 2^k possible distributions of sign. The cross-products come in pairs and hence eliminate each other. Hence we have

$$(3.16) \qquad \sum_{1\le i\le 2^k} (s_i - \frac{A}{2})^2 = 2^{k-2} \sum_{j=1}^{k} a_j^2 < 2^{k-2} kn^2 .$$

If $\left| s_i - \frac{A}{2} \right| \ge \sqrt{k}\, n$ for more than 2^{k-1} of the subset sums, we would have $\sum_{1\le i\le 2^k} (s_i - \frac{A}{2})^2 > 2^{k-1} (\sqrt{k}\, n)^2$, which contradicts (3.16). Hence we must have at least 2^{k-1} distinct numbers in a range less than $2\sqrt{k}\, n$. Therefore $2^{k-2} < \sqrt{k}\, n$ from which it follows that $(k-2) < \frac{1}{2}\log_2 k + \log_2 n$. Since $k \le 2\log_2 n$ we must have

$$(3.17) \qquad k-2 < \frac{1}{2}\log_2(2\log_2 n) + \log_2 n .$$

Hence $\qquad k < \log_2 n + \frac{1}{2}\log_2\log_2 n + \frac{5}{2}$.

CHAPTER IV

<u>Introduction.</u> In this chapter we consider problems of the following type: can every integer be represented as an element of one of a finite number of arithmetic progressions, the common differences of these progressions all being distinct?

Consider a finite set of arithmetic progressions P_i, $(1 \leq i \leq k)$, where the elements of P_i are integers x of the form $x \equiv a_i (\mathrm{mod}\ n_i)$. Suppose $1 < n_1 < n_2 \ldots < n_k$. We call such a set a covering set of congruences if every integer m satisfies at least one of the congruences. We use the notation $a(n)$ to denote the arithmetic progression of integers x satisfying $x \equiv a (\mathrm{mod}\ n)$.

We list several examples of such covering sets of congruences. The fourth example is due to Erdös [7]. Davenport [6] and Swift [31] have constructed further examples of covering sets of congruences.

(1)	(2)	(3)	(4)
0(2)	0(2)	0(2)	0(3)
0(3)	0(3)	0(3)	0(4)
1(4)	1(4)	1(4)	0(5)
5(6)	1(6)	3(8)	1(6)
7(12)	11(12)	7(12)	6(8)
		23(24)	3(10)
			5(12)
			11(15)
			7(20)
			10(24)
			2(30)
			34(40)
			59(60)
			98(120)

To prove that these sets do, in fact, form covering sets of congruences it suffices to show, in each case, that all possible residue classes $(\mathrm{mod}\ n_k)$ are accounted for and this is readily verified.

We proceed to discuss some results and unsolved problems in this connection.

Erdös and Mirsky [10] have shown that

$$(4.1) \qquad \sum_{i=1}^{k} \frac{1}{n_i} > 1$$

As the asymptotic density of integers x satisfying $x \equiv a (\mathrm{mod}\ n)$ is $\frac{1}{n}$ we may immediately conclude that $\sum_{i=1}^{k} \frac{1}{n_i} \geq 1$. The proof of strict inequality mentioned above uses an analytic approach and will not be given here.

We say that a covering set is of order M if $n_1 = M$. Covering sets of order as large as six are known to exist. Swift [31] has shown that for certain small M there exist classes of covering congruences. In particular for $M = 2$ if p is an arbitrary odd prime and g an arbitrary singly even primitive root of p then the set $g^{i-1}\ (2^i)$, $g^{i-1}\ (2^{i-1}p)$ and $0(2^{p-1}p)$, $(1 \leq i \leq p-1 \leq k)$, forms a covering set of congruences.

PROOF:

It is necessary that the sum of the reciprocals of the moduli involved totals $M(p)$, where $M(p) > 1$ for p any odd prime. The sum is

$$(4.2) \qquad \sum_{i=1}^{p-1} \frac{1}{2^i} + \sum_{i=1}^{p-1} \frac{1}{2^{i-1}p} + \frac{1}{2^{p-1}p} = 1 + \frac{2}{p} - \left(\frac{1}{2}\right)^{p-1} \frac{p+1}{p} = M(p) .$$

In order that $\frac{2}{p} - \left(\frac{1}{2}\right)^{p-1} \frac{p+1}{p}$ be positive we must have $\frac{2}{p} > \left(\frac{1}{2}\right)^{p-1} \frac{p+1}{p}$ which implies $p + 1 < 2^p$. This inequality is seen to hold for the range of p considered.

Putting $i = 1$ in $g^{i-1}(2^i)$ produces $1(2)$ which disposes of all odd integers. It remains to show that all even integers are produced. To prove this, we first show that the sum of the reciprocals of the moduli which are producing even integers is greater than $\frac{1}{2}$, the asymptotic density of the even integers. However some of the congruences can be solved simultaneously so that there is some overlap. We evaluate this overlap. Subtracting this quantity from the sum of the reciprocals of the moduli in question gives the number $\frac{1}{2}$. Hence the set of congruences accounts for all the even integers.

Putting $i = 1$ in $g^{i-1}(2^{i-1}p)$ produces $1(p)$. This congruence produces an equal number of even and odd integers. The asymptotic density of the even numbers it produces is $\frac{1}{2p}$.

The density of the numbers being considered, all of which are even, is thus

$$(4.3) \qquad M(p) - \frac{1}{2} - \frac{1}{2p} = \frac{1}{2} + \frac{3}{2p} - \left(\frac{1}{2}\right)^{p-1} \frac{p+1}{p} .$$

In order that $\frac{3}{2p} - \left(\frac{1}{2}\right)^{p-1} \frac{p+1}{p}$ be positive we must have $(p+1) < 3.2^{p-2}$, an inequality which is seen to hold for the range of p considered.

It remains to evaluate the overlap and to show that it totals $\frac{3}{2p} - \left(\frac{1}{2}\right)^{p-1} \frac{p+1}{p}$.

We are concerned with the following set of congruences:

(i) $\qquad g^{i-1}(2^i)$ for $2 \leq i \leq p-1$

(ii) $\qquad g^{i-1}(2^{i-1}p)$ for $1 \leq i \leq p-1$

(iii) $\qquad 0(2^{p-1}p)$.

We consider two types of overlap; within the same class (internal) and between classes (external). We show that overlap occurs only externally and just between classes (i) and (ii)

Obviously there is no internal overlap in (iii). Consider any two progressions from (i), say $g^{j-1}(2^j)$ and $g^{m-1}(2^m)$ where we may assume, without loss of generality, that $2 \leq j \leq m \leq p-1$. For overlap to exist, we would have to have the g.c.d. $(2^j, 2^m) \mid (g^{m-1}-g^{j-1})$. Now $(2^j, 2^m) = 2^j$ and $(g^{m-1}-g^{j-1}) = g^{j-1}(g^{m-j}-1)$. The number $(g^{m-j}-1)$ is odd for $m-j \geq 1$ because g is even so overlap can occur if and only if $m=j$. However if $m=j$ we are considering one and the same congruence. Hence there is no internal overlap in (i). Now consider any two progressions from (ii), say $g^{j-1}(2^{j-1}p)$ and $g^{m-1}(2^{m-1}p)$ where we may again assume, without loss of generality, that $1 \leq j \leq m \leq p-1$. Now $(2^{j-1}p, 2^{m-1}p) = 2^{j-1}p$ and $(g^{m-1}-g^{j-1}) = g^{j-1}(g^{m-j}-1)$. Certainly $2^{j-1}p$ divides g^{j-1} but $p \nmid (g^{m-j}-1)$. If we had $mp = (g^{m-j}-1)$ then $g^{m-j} \equiv 1 \pmod{p}$. However g is a primitive root of p and hence $g^s \not\equiv 1 \pmod{p}$ for $s < \phi(p) = p-1$ and $(m-j) \leq p-2$ always. Hence there is no internal overlap in (ii).

We now consider the question of external overlap. Consider the progressions $g^{i-1}(2^i)$ and $0(2^{p-1}p)$. We have $(2^i, 2^{p-1}p) = 2^i$ and $g^{i-1} - 0 = g^{i-1}$. Now $2^i \nmid g^{i-1}$ and so we have no overlap between (i) and (iii). Consider the progressions $g^{i-1}(2^{i-1}p)$ and $0(2^{p-1}p)$. We have $(2^{i-1}p, 2^{p-1}p) = 2^{i-1}p$ and $g^{i-1}-0 = g^{i-1}$. Now $2^{i-1}p \nmid g^{i-1}$ and so we have no overlap between (ii) and (iii). Finally we consider the possibility of there being external overlap between pairs of progressions, one from (i) and one from (ii). In general we have $g^{j-1}(2^j)$ and $g^{m-1}(2^{m-1}p)$ where $2 \leq j \leq p-1$ and $1 \leq m \leq p-1$. If $m=j$ we have

$(2^j, 2^{m-1}p) = 2^{m-1}$ and $(g^{j-1}-g^{m-1}) = 0$. Now $2^{j-1} \mid 0$ so that there exists overlap of density $\frac{1}{2^j p}$. Hence the total overlap obtained in this way will be $\sum_{j=2}^{p-1} \frac{1}{2^j p}$. If $m > j$ we have $(2^j, 2^{m-1}p) = 2^j$ and $(g^{m-1}-g^{j-1}) = g^{j-1}(g^{m-j}-1)$. Now $2^j \nmid g^{j-1}(g^{m-j}-1)$ so that we have no overlap. In the last case, $j > m$, we have $(2^j, 2^{m-1}p) = 2^{m-1}$ and $(g^{j-1}-g^{m-1}) = g^{m-1}(g^{j-m}-1)$. Now $2^{j-1} \mid g^{m-1}(g^{j-m}-1)$ so that we have overlap. We now compute the total overlap for this case by assigning all possible values to m and determining the density of overlap as j varies. Thus when $m = 1$ we have $2 \leq j \leq p-1$. For any j value the density of overlap is $\frac{1}{2^j p}$. Hence the total contribution is $\sum_{j=2}^{p-1} \frac{1}{2^j p}$. When $m = 2$ we have $3 \leq j \leq p-1$ and the total contribution is $\sum_{j=3}^{p-1} \frac{1}{2^j p}$. Continuing in this way we find that the total density of overlap from cases $j > m$ is

$$\sum_{j=2}^{p-1} \frac{1}{2^j p} + \sum_{j=3}^{p-1} \frac{1}{2^j p} + \cdots + \sum_{j=p-2}^{p-1} \frac{1}{2^j p} + \frac{1}{2^{p-1} p} .$$

Hence total overlap, considering all sources, is

$$(4.4) \qquad 2 \sum_{j=2}^{p-1} \frac{1}{2^j p} + \sum_{j=3}^{p-1} \frac{1}{2^j p} + \cdots + \sum_{j=p-2}^{p-1} \frac{1}{2^j p} + \frac{1}{2^{p-1} p} .$$

As $\sum_{j=\alpha}^{p-1} \frac{1}{2^j p} = \frac{1}{2^{\alpha-1} p} \left(1 - \left(\frac{1}{2}\right)^{p-\alpha}\right)$ we obtain

$$\frac{1}{2p}\left(1-\left(\frac{1}{2}\right)^{p-2}\right)+\frac{1}{2p}\left(1-\left(\frac{1}{2}\right)^{p-2}\right)+\frac{1}{2^2p}\left(1-\left(\frac{1}{2}\right)^{p-3}\right)+\cdots$$

$$\cdots+\frac{1}{2^{p-2}p}\left(1-\left(\frac{1}{2}\right)^{p-(p-1)}\right)=\frac{1}{2^{p-1}p}\left((2^{p-2}-1)+(2^{p-2}-1)+\cdots+(2^{p-(p-1)}-1)\right)$$

$$=-\frac{(p-1)}{2^{p-1}p}+\frac{2^1+2^2+\cdots+2^{p-3}+2^{p-2}+2^{p-2}}{2^{p-1}p}$$

$$=-\left(\frac{1}{2}\right)^{p-1}+\frac{1}{2^{p-1}p}+\frac{3}{2p}-\frac{1}{2^{p-2}p}=\frac{3}{2p}-\left(\frac{1}{2}\right)^{p-1}\frac{p+1}{p}.$$

Hence the result follows.

We have shown that $M(p) = 1 + \frac{2}{p} - \left(\frac{1}{2}\right)^{p-1} \frac{(p+1)}{p}$ and know that $M(p) > 1$ for all possible p. However we note that for sufficiently large p and arbitrary $\epsilon > 0$ we have $M(p) < 1 + \epsilon$.

As a simple example of the type of covering set being discussed, let us choose $p = 5$, $g = 2$. We obtain:

1(2)	1(5)	0(80)
2(4)	2(10)	
4(8)	4(20)	
8(16)	8(40)	

There are several unsolved problems in connection with this general problem. It is not known whether there exist covering sets of order greater than six. More generally, Erdös [7] has conjectured that there exist covering sets of arbitrarily large order. It is also not known whether there exist systems in which the moduli are all odd.

CHAPTER V

Introduction. In this chapter we begin by introducing the concept of "addition chain", as defined by Scholz [29]. We then discuss various results due to Brauer [4] and Utz [32] in this connection and end the chapter by mentioning some unsolved problems concerning addition chains.

We define an addition chain for any positive integer n to be a set of distinct positive integers $1 = a_0 < 2 = a_1 < a_2 < \ldots < a_r = n$ such that every element a_ρ, $(1 \leq \rho \leq r)$, can be written as a sum $a_\sigma + a_\tau$, $(1 \leq \sigma \leq \tau \leq \rho - 1)$, of two preceding elements of the set. Clearly, $a_1 = 2$, $a_3 = 3$ or 4.

We list three possible addition chains for $n = 10$:

1	1	1
2	2	2
4	4	3
8	6	6
10	10	9
		10

An addition chain $1 < 2 < a_2 < \ldots < a_r = n$ is said to have "length" r. By an addition chain of minimal length $\ell = \ell(n)$, Scholz [29] understands the smallest ℓ for which there exists an addition chain $1 < 2 < a_2 < \ldots < a_\ell = n$.

Scholz [29] published the following as problems:

(5.1) $\quad (m + 1) \leq \ell(n) \leq 2m \quad$ for $\quad 2^m + 1 \leq n \leq 2^{m+1}$, $m \geq 1$.

(5.2) $\quad \ell(ab) \leq \ell(a) + \ell(b)$

(5.3) $\quad \ell(2^{m+1}-1) \leq m + \ell(m + 1)$

Brauer [4] has established (5.1) and (5.2) and we give his proofs:

Proof of (5.1). It is clear, from the definition, that in any addition chain for n we have $a_\rho \leq 2a_{\rho-1}$, $(1 \leq \rho \leq r)$. Thus it will require at least $(m+1)$ steps to produce an element which exceeds 2^m. Hence $\ell(n) \geq (m+1)$ for the range of n being considered. To establish the other side of the inequality, let us express n in the binary scale. We have

$$(5.4) \qquad n = \sum_{i=1}^{k} 2^{\nu_i} \quad \text{where} \quad 0 \leq \nu_1 < \nu_2 < \ldots < \nu_k = m, \ (2 \leq k \leq m+1),$$

for $2^m + 1 \leq n \leq (2^{m+1}-1)$.

An addition chain for n is

$$(5.5) \qquad 1 < 2^1 < 2^2 < \ldots < 2^m < 2^m + 2^{\nu_1} < 2^m + 2^{\nu_1} + 2^{\nu_2} < \ldots < \sum_{i=1}^{k} 2^{\nu_i} = n.$$

The length of such a chain is $m + k - 1 \leq 2m$. If $n = 2^{m+1}$, $\ell(n) = m+1$ so that $\ell(n) \leq 2m$ for all values of n being considered.

Proof of (5.2). Let $1, 2, a_2, \ldots a_r = a$ be an addition chain for a with $r = \ell(a)$. Let $1, 2, b_2, \ldots b_s = b$ be an addition chain for b with $s = \ell(b)$. Consider the set of distinct positive integers

$$(5.6) \qquad 1, 2, a_2, \ldots a_r, a_r b_1, a_r b_2, \ldots a_r b_s = ab .$$

By assumption, $b_\rho = b_\sigma + b_\tau$, $(1 \leq \rho \leq s)$, $(1 \leq \sigma \leq \tau \leq \rho - 1)$, so that $a_r b_\rho = a_r b_\sigma + a_r b_\tau$. Hence (5.6) is an addition chain of length $(r+s)$ for ab. Thus we have

$\ell(ab) \leq (r+s) = \ell(a) + \ell(b)$.

It is not known at present whether (5.3) is true. Utz [32] has shown that

(5.7) $\qquad \ell(2^q-1) \leq q + \ell(q) - 1 = 2^s(2^n+1) + n+s$

$\qquad$ for $q = 2^s(2^n + 1)$, $\quad s, n \geq 0$.

Brauer [4] has a result in this direction where the addition chains are 'restricted' in a certain way. A 'special addition chain' for any positive integer n is an addition chain $1 < 2 < a_2 < \ldots < a_r = n$ such that every element a_ρ, $(1 \leq \rho \leq r)$, can be written as a sum $a_{\rho-1} + a_\sigma$, $(1 \leq \sigma \leq \rho-1)$. We denote by $\ell^*(n)$ the length of the shortest special addition chain for n. Clearly $\ell(n) \leq \ell^*(n)$ for any value of n. We now prove that

$$\ell^*(2^{m+1}-1) \leq m + \ell^*(m+1), \quad m \geq 3.$$

PROOF:

The result is easily seen to hold for $m = 0, 1$ and 2. For $m \geq 3$, $1, 2, 4, 5, 6, \ldots, (m + 1)$ is a special addition chain for $(m + 1)$ so that $\ell^*(m + 1) \leq (m-1)$. Let us consider a special addition chain of minimal length for $(m + 1)$ having the form

(5.8) $\qquad 1 < 2 < a_2 < \ldots < a_k = m + 1, \quad k = \ell^*(m + 1)$.

We construct numbers of the form $2^{a_\lambda}-1$, $(0 \leq \lambda \leq k)$. Further, we multiply each number of this form, except $(2^{a_k}-1)$, successively $(a_{\lambda+1} - a_\lambda)$ times by 2, producing a total of $\sum_{\lambda=0}^{k-1} (a_{\lambda+1} - a_\lambda) = m$ numbers. Consider the set of distinct positive integers

(5.9) $\qquad 1, 2, (2^{a_1}-1), 2^1(2^{a_1}-1), \ldots 2^{a_2-a_1}(2^{a_1}-1), (2^{a_2}-1), 2^1(2^{a_2}-1),$

$\ldots 2^{a_3-a_2}(2^{a_2}-1), \ldots, (2^{a_{k-1}}-1), 2^1(2^{a_{k-1}}-1), \ldots 2^{a_k-a_{k-1}}(2^{a_{k-1}}-1),$

$(2^{a_k}-1) = 2^{m+1}-1$.

A number of the form $(2^{a_\rho}-1)$, $(1 \leq \rho \leq k)$, is always preceded by a number of the form $2^{a_\rho - a_{\rho-1}}(2^{a_{\rho-1}}-1)$. The number $(2^{a_\rho}-1) - 2^{a_\rho - a_{\rho-1}}(2^{a_{\rho-1}}-1) = 2^{a_\rho - a_{\rho-1}}-1$ is an element of (5.9) because $(a_\rho - a_{\rho-1})$ is an element of (5.8). Hence (5.9) is a special addition chain for $2^{m+1}-1$. We have

$$(5.10) \qquad \ell^*(2^{m+1}-1) \leq m + \ell^*(m+1) \leq (2m-1), \quad m \geq 3.$$

Another result due to Brauer [4] is the following:

THEOREM 5.1:

For any non-negative integer s and any positive integer r we have

$$(5.11) \qquad \ell(n) \leq (r+1)s + 2^r-2 \quad \text{for} \quad 2^{rs} \leq n < 2^{r(s+1)}.$$

PROOF:

Let us first consider the case $r = 1$, s being arbitrary. We must have $\ell(n) \leq 2s$ for $2^s \leq n < 2^{s+1}$. Since $\ell(2^s) = s$ we see that the result holds by making use of (5.1). Consider $r > 1$ to be arbitrary and fixed. We prove the remaining cases to which (5.11) is applicable using induction on s. The case $s = 0$ requires that $\ell(n) \leq 2^r-2$ for $1 \leq n < 2^r$. The set of distinct positive integers $1, 2, 3, \ldots, (2^r-1)$ forms an addition chain for any n in the range considered. We now assume that for any n such that $2^{rt} \leq n < 2^{r(t+1)}$, $(1 \leq t \leq s-1)$, we may form an addition chain containing at most $(r+1)t + 2^r-1$ elements, the first (2^r-1) elements being the numbers $1, 2, 3, \ldots, (2^r-1)$. We complete the induction by considering the

case $t = s$. We have $2^{rs} \leq n < 2^{r(s+1)}$. Dividing n by 2^r we obtain

$$(5.12) \qquad n = a\,2^r + b \quad \text{for} \quad 2^{r(s-1)} \leq a < 2^{rs}, \; 0 \leq b < 2^r .$$

By the induction hypothesis there exists an addition chain $1, 2, 3, \ldots, 2^r-1, a_{2^r-1}, \ldots, a_{\alpha-1}, a_\alpha = a$ for a having the form shown and having length not exceeding $(r+1)(s-1) + 2^r-2$. If $b > 0$ this addition chain contains b. The following set of distinct positive integers forms an addition chain for n:

$$(5.13) \qquad 1, 2, 3, \ldots, 2^r-1, a_{2^r-1}, \ldots, a_{\alpha-1}, a, 2^1a, 2^2a, \ldots 2^ra, \quad 2^ra + b = n .$$

The length of this addition chain is at most $((r+1)(s-1) + 2^r-2) + r+1 = (r+1)s + 2^r-2$ which completes the proof.

Using (5.11) we now prove

$$(5.14) \qquad \lim_{n\to\infty} \frac{\ell(n)}{\log_2 n} = 1 .$$

In (5.11) we have $2^{rs} \leq n$ so that $s \leq \frac{1}{r} \log_2 n$. Thus the first portion of (5.11) may be written as

$$(5.15) \qquad \ell(n) \leq (1 + \frac{1}{r}) \log_2 n + 2^r-2 .$$

Let us insist that n be in the range $2^m \leq n < 2^{m+1}$ so that $2^{rs} \leq 2^m \leq n < 2^{m+1} \leq 2^{r(s+1)}$. For non-trivial cases, the value of r must be in the range $1 \leq r \leq m$ and we have

$$(5.16) \qquad \ell(n) \leq \min_{r=1,2,\ldots,m} ((1 + \frac{1}{r}) \log_2 n + 2^r-2)$$

Taking $r = [\log\log n] + 1$ provides a "near-minimum" value for the

expression $\left((1+\frac{1}{r})\log_2 n + 2^r - 2\right)$. Using this value of r in (5.15) we may write

(5.17) $$\ell(n) < \left(1 + \frac{1}{\log\log n}\right)\log_2 n + 2^{\log\log n + 1}$$

From (5.17) it follows easily that

(5.18) $$\ell(n) < \log_2 n \left(1 + \frac{1}{\log\log n} + \frac{2\log 2}{(\log n)^{1-\log 2}}\right)$$

Also, since $2^m \leq n < 2^{m+1}$, we have, using (5.1),

(5.19) $$\ell(n) \geq m > \log_2 n - 1 .$$

From (5.18) and (5.19) it follows that $\lim_{n \to \infty} \frac{\ell(n)}{\log_2 n} = 1$.

The following questions have been asked by Utz [32]:

(i) is it true that $\ell(p) < \ell(2p)$ for all $p > 0$?

(ii) if we denote by $S(n)$ the number of solutions of $\ell(x) = n$ can it be shown that $S(n) < S(n+1)$ for all $n > 0$?

These questions appear to be unsolved at the present time.

CHAPTER VI

Introduction. In this chapter we discuss some results of Kelly [13] concerning the possibility of representing all positive integers as a sum of a restricted number of distinct elements of a given sequence.

We begin with three definitions.

(i) A basis of order h is a set of non-negative integers such that every positive integer can be expressed as a sum of h elements of the set, h being the smallest number for which this is true.

(ii) An asymptotic basis of order h is a set of non-negative integers containing zero such that every sufficiently large positive integer can be expressed as a sum of h or fewer elements of the set, h being the smallest number for which this is true.

(iii) A restricted basis of order h is a set of non-negative integers such that every sufficiently large positive integer can be expressed as a sum of h or fewer elements of the set without repetitions, h being the smallest number for which this is true.

We give some illustrative examples and make some clarifying remarks in connection with the above definitions.

By Lagrange's theorem, the set of squares is a basis of order 4 while by a theorem of Pall [20] this set is a restricted basis of order 5. It is not the case that every basis or every asymptotic basis is a restricted basis, as may be seen from the following counter-example, due to Bateman [13]. Consider the set consisting of 1 together with all non-negative multiples of a

positive integer h. i.e. $0, 1, h, 2h, \ldots$

This set is a basis of order h. Any positive integer m may be written as $m = rh + s$ where r and s are non-negative integers, not simultaneously zero, and $s \leq (h-1)$. m requires $(s+1)$ elements for its representation. One element is rh, which is in the set, and the remaining s elements are each the number 1. If $s = h-1$ we have m expressed as a sum of h elements. For $s < (h-1)$ we add the necessary number of zeros to express m as a sum of h elements of the set. Thus we see that the set is a basis of order h. If $h = 2$ it is obvious that the set $0, 1, 2, 4, 6, \ldots$ also forms a restricted basis of order h. However for $h > 2$ the set $0, 1, h, 2h, \ldots$ is not a restricted basis of any order because elements of the form $th-1$, where t is any positive integer, cannot be represented as a sum of elements of the set without there being repetition.

Kelly's results concern bases of order 2 and may be stated as follows:

THEOREM 6.1:

Given any arbitrary basis of order 2 it is a restricted basis of order less than or equal to 4.

THEOREM 6.2:

An asymptotic basis of order 2 is a restricted basis of order at most 3 if the value of its counting function is, for a suitable positive constant C, larger than $\dfrac{Cx}{\log\log x}$ for all sufficiently large x. The counting function, $A(x)$, of a set of integers A is the number of integers in the set which do not exceed x, x being a non-negative real number.

It may be the case that every basis, or even every asymptotic

basis, of order 2 is a restricted basis of order at most 3, but the problem of proving this has not yet been solved. We show, by means of an example, that if the above statement were true it would be the best possible result. Consider the set of non-negative integers whose representations in the ternary scale require only the digits 0 and 1. We prove that this set is a basis of order 2 which is not a restricted basis of order 2. From this result it follows that there is at least one asymptotic basis of order 2 which is a restricted basis of order at least 3. A similar statement holds with regard to bases of order 2. The set under discussion is represented, using numbers of the ternary scale only, as

0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111, ...

Writing these numbers in the decimal scale, we obtain

0, 1, 3, 4, 9, 10, 12, 13, 27, 28, 30, 31, 36, 37, 39, 40, ...

It is easily seen that in the above set the numbers $\frac{3^k-1}{2}$ and 3^k, for all non-negative k, are adjacent. Hence positive integers of the form (3^k-1) cannot be expressed as a sum of two or fewer elements of the set without repetitions. As we may find arbitrarily large integers of this form, the set cannot be a restricted basis of order 2. We now prove that the set is a basis of order 2. Certainly we have a set of non-negative integers. The proof goes by induction. It is sufficient to show that, given all the elements of the set which are less than 3^n, we are able to represent each positive integral x, $1 \leq x \leq (3^n-1)$ as a sum of two of the elements at our disposal, n being any non-negative integer. When $n = 1$ we have the elements 0 and 1 at our disposal. The positive integers 1 and 2 may be represented as $1 = 0+1$ and $2 = 1+1$. When $n = 2$ we have the elements 0, 1, 3 and 4 at our disposal.

The positive integer less than $3^n = 3^2 = 9$ may be represented as $1 = 0+1$, $2 = 1+1$, $3 = 0+3$, $4 = 0+4$, $5 = 1+4$, $6 = 3+3$, $7 = 3+4$ and $8 = 4+4$. We now assume that the result holds for the case $n = k$. i.e. if we have the elements of the set which are less than 3^k then it is possible to represent each positive integral x, $1 \leq x \leq (3^k-1)$ in the required manner. It remains to show that the above statement is true for k replaced by $(k+1)$. We now have at our disposal the elements

$$0,\ 1,\ 3^1,\ 3^1+1,\ 3^2,\ 3^2+1,\ 3^2+3^1,\ 3^2+3^1+1,\ \ldots\ \frac{3^{k+1}-1}{2} = \sum_{r=0}^{k} 3^r$$

of the set. By the induction hypothesis, the numbers less than 3^k are representable in the appropriate manner. Thus we are concerned with those positive integers x where $3^k \leq x \leq (3^{k+1}-1)$. Any integer in this range consists of $(k+1)$ ternary digits. If we exclude the digit on the extreme left, which must be a 1 or a 2, the remaining k ternary digits form a number which may be obtained as a sum of two of the elements we have at our disposal. To obtain the $(k+1)$ digit number we simply append a ternary 1 to either one or both of the numbers whose sum is the k-digit number. For example if $k = 5$ and the number we are trying to produce is 211012 we may write $11012 = 10010 + 01001$. Then $211012 = 110010 + 101001$. The numbers are elements of the set because they consist only of ternary 0's and 1's and all possible configurations of zeros and ones appear in the set. Hence the statement is true for $n = (k+1)$ and the induction is complete. Hence the set is a basis of order 2.

In order to prove Theorem 6.1 we first state and prove two lemmas. In this work we denote by A any basis of order 2. The elements of A we denote by a_i, $i = 1, 2, 3, \ldots$. By a'

we mean the smallest element in A which is larger than a. For an arbitrary integer x, $\rho(x)$ denotes the number of representations of x as a sum of two elements of A. The representations $x = a_i + a_j$ and $x = a_j + a_i$ are regarded as distinct when $i \neq j$.

LEMMA 6.3:

If A is a basis of order 2, there exists an even integer x such that $\rho(x) \geq 4$.

LEMMA 6.4:

If A is a basis of order 2, then either there exists an odd integer y such that $\rho(y) \geq 4$ or A is one of the two sets $(0, 1, 3, \ldots, 2n+1, \ldots)$, $(0, 1, 2, 4, \ldots, 2n, \ldots)$.

PROOF OF LEMMA 6.3:

We assume that every even number has no more than three representations as a sum of 2 integers of a basis, A, of order 2 and obtain a contradiction. In order that 1 be representable as a sum of two elements of A we must have $0 = a_1$, $1 = a_2$. If $a_3 \geq 4$ then we cannot represent 3 as a sum of two elements of A. Hence $a_3 < 4$. We consider all possible cases.

CASE 1. $a_3 = 2$, $a_4 = 3$. $3' = 4$ implies $\rho(4) > 3$. Hence $3' > 4$. If $3' = 5$ then $5' = 9$ because $5' < 9$ implies $\rho(8) > 3$ and $5' > 9$ implies $\rho(9) = 0$. Further $9' = 13$ because $9' < 13$ implies $\rho(12) > 3$ and $9' > 13$ implies $\rho(13) = 0$. We now have 0, 1, 2, 3, 5, 9, 13 and $\rho(14) > 3$. Hence $3' > 5$. If $3' = 6$ then $6' \geq 9$ because $6' < 9$ implies $\rho(8) > 3$. If $6' = 9$ then $9' = 13$ because $9' < 13$ implies $\rho(12) > 3$ and $9' > 13$ implies $\rho(13) = 0$. $13' = 17$ because $13' < 17$ implies $\rho(16) > 3$ and $13' > 17$ implies $\rho(17) = 0$. $17' = 21$ because

$17' < 21$ implies $\rho(20) > 3$ and $17' > 21$ implies $\rho(21) = 0$. We now have $0, 1, 2, 3, 6, 9, 13, 17, 21$ and $\rho(20) > 3$. Hence $6' > 9$. $6' = 10$ because $6' > 10$ implies $\rho(10) = 0$. $10' \geq 13$ because $10' < 13$ implies $\rho(12) > 3$. $10' < 15$ because $10' \geq 15$ implies $\rho(14) = 0$. $10' = 13$ implies $\rho(16) > 3$. $10' = 14$ implies $\rho(16) > 3$. Hence $3' \neq 6$. Thus $3' = 7$ because $3' > 7$ implies $\rho(7) = 0$. $7' = 11$ because $7' < 11$ implies $\rho(10) > 3$ and $7' > 11$ implies $\rho(11) = 0$. $11' = 15$ because $11' < 15$ implies $\rho(14) > 3$ and $11' > 15$ implies $\rho(15) = 0$. We now have $0, 1, 2, 3, 7, 11, 15$ and $\rho(18) > 3$. Hence A cannot contain both 2 and 3.

CASE 2. $a_3 = 2$, $a_4 \geq 4$. If $2' = 4$ then $4' = 7$ because $4' < 7$ implies $\rho(6) > 3$ and $4' > 7$ implies $\rho(7) = 0$. If $7' = 8$ then $\rho(8) > 3$. If $7' = 9$ we have $0, 1, 2, 4, 7, 9$. Then 10 is not in A for otherwise $\rho(10) > 3$. Also 12, 14, 15 and 16 are not in A, for otherwise $\rho(16) > 3$. If $9' \geq 13$ then $\rho(12) = 0$. Hence $9' = 11$. If $11' = 13$ then $\rho(20) > 3$. If $11' > 17$ then $\rho(17) = 0$. Thus $11' = 17$. We now have $0, 1, 2, 4, 7, 9, 11, 17$ and $\rho(13) > 3$. Hence $7' \neq 9$. $7' = 10$ because $7' > 10$ implies $\rho(10) = 0$. 11 and 12 are not in A for otherwise $\rho(12) > 3$. $10' = 13$ implies $\rho(14) > 3$. Hence $10' \geq 14$. But now $\rho(13) = 0$. Hence $2' \neq 4$. Thus $2' = 5$ for otherwise $\rho(5) = 0$. Now $5' \neq 6$ for then $\rho(6) > 3$. If $5' = 7$ then $7' \geq 9$ because $7' = 8$ implies $\rho(8) > 3$. If $7' = 9$ then 10, 11 and 12 cannot be in A for otherwise $\rho(12) > 3$. If 13 is in A, $\rho(14) > 3$. Hence $9' \geq 14$. But now $\rho(13) = 0$. Hence $7' > 9$. If $7' \leq 12$ then $\rho(12) > 3$. But $7' > 11$ implies $\rho(11) = 0$. Hence $5' \neq 7$. Hence $5' = 8$ for

otherwise $\rho(8) = 0$. $8' \geq 11$ because $8' < 11$ implies $\rho(10) > 3$. $8' = 11$ because $8' > 11$ implies $\rho(11) = 0$. $11' = 12$ implies $\rho(12) > 3$. Hence $11' \geq 13$. If $11' = 13$ then 14, 15, 16 cannot lie in A, for otherwise $\rho(16) > 3$. Also 17 cannot be in A, for then $\rho(18) > 3$. But now $\rho(17) = 0$. Hence $11' \geq 14$. $11' > 14$ implies $\rho(14) = 0$ so $11' = 14$. We now have 0, 1, 2, 5, 8, 11, 14 and so $\rho(16) > 3$. Hence we cannot have $2 = a_3$, $a_4 \geq 4$.

CASE 3. $a_3 = 3$ $3' = 4$ implies $\rho(4) > 3$. Hence $3' > 4$. Hence $3' = 5$ for otherwise $\rho(5) = 0$. $5' \neq 6$ for then $\rho(6) > 3$. Hence $5' = 7$ for otherwise $\rho(7) = 0$. But now $\rho(8) > 3$. Hence the case $a_3 = 3$ cannot occur.

Thus we have obtained a contradiction which proves Lemma 6.3.

PROOF OF LEMMA 6.4:

Let A be a basis of order 2. $a_1 = 0$ and $a_2 = 1$ as before. Clearly every odd positive integer has at least two representations as the sum of two elements of A. We assume that every odd positive integer has exactly two such representations.

CASE 1. $a_3 = 2$. We show that the rest of the numbers of A are even. Suppose the contrary. Let $2m+1$, $m \geq 1$, be the smallest odd number, apart from 1, in A. Then we must have the numbers 2, 4, ... $(2m-2)$ as elements of A for otherwise we would not be able to represent the odd numbers 3, 5, ... $(2m-1)$. If $2m$ is in A then $\rho(2m+1) > 2$, contrary to assumption. Hence $2m$ is not in A. We now have $2m+3 = (2m+1) + 2$, $2m+5 = (2m+1) + 4$, ... $4m-1 = (2m+1) + (2m-2)$ so that every odd number not exceeding $(4m-1)$ has exactly two representations. Thus $(2m+1)' > (4m-1)$. Now in

A the elements not exceeding $(4m-1)$ are $0, 1, 2, 4, \ldots (2m-2), (2m+1)$. Consider the positive integer $(4m-2)$. For $m \geq 3$, $\rho(4m-2) = 0$. If $m = 1$ we have $(4m-2) = 2$. But we also have $2m+1 = 3$ so that $\rho(3) > 2$, contrary to assumption. If $m = 2$, $(2m-2) = 2$ and $(2m+1) = 5$ so that the elements in $A < 4m = 8$ are $0, 1, 2, 5$. $5' = 8$ for otherwise $\rho(8) = 0$. If 9 is in A then $\rho(9) > 2$. Hence 9 is not in A. 11 is not in A, for otherwise $\rho(13) > 2$. Thus $8' = 10$ for otherwise $\rho(11) = 0$. We now have $0, 1, 2, 5, 8, 10$. If 12 or 13 is in A then $\rho(13) > 2$. Hence 12 and 13 are not in A. 14 is not in A, for otherwise $\rho(15) > 2$. But now $\rho(14) = 0$. Hence the case $m = 1$ is also excluded. Hence our assumption has led to a contradiction which means that 1 is the only odd element of A. We find that the set $(0, 1, 2, 4, 6, \ldots, 2n, \ldots)$ is the only basis of order 2 which contains the number 2 and in which every odd number has exactly two representations as the sum of two elements of the set.

CASE 2. $a_3 = 3$. We show that the rest of the elements of A are odd. Suppose the contrary. Let $2m$, $m \geq 2$, be the smallest even element of A. Then the odd positive integers $3, 5, \ldots (2m-1)$ must be elements of A. All positive integers which are less than $(4m+1)$ are representable and so it must be the case that $(2m)' \geq 4m$. If $(2m)' = 4m$ then $(4m)' > 4m+2$ as otherwise $\rho(4m+1) > 2$ or $\rho(4m+3) > 2$. But now $\rho(4m+2) = 0$. If $(2m)' \geq 4m+2$ then $\rho(4m+2) = 0$. Hence $(2m)' = 4m+1$. We now have the elements $0, 1, 3, 5, \ldots (2m-1), 2m, 4m+1$ in A. As we require representations for the odd numbers $4m+3, 4m+5, \ldots (6m-1)$ we shall have to have these numbers as elements of A. We cannot have any even numbers in the interval $[4m+2, 6m-2]$ as elements of A because this would

be too many representations for some larger odd number. For instance, $(4m+2)$ in A would make $\rho(6m+1) > 2$. We now have $0, 1, 3, 5, \ldots (2m-1), (2m), (4m+1), (4m+3), \ldots (6m-1)$. All integers not exceeding $(8m-1)$ may now be represented. Hence there are no integers in A in the range $[6m, 8m-1]$. $8m$ is in A for otherwise $\rho(8m) = 0$. All numbers not exceeding $10m$ now have representations so that there are no integers in A in the range $[8m+1, 10m-1]$. We must have either $(8m)' = 10m$ or $(8m)' = 10m+1$ for otherwise $\rho(10m+1) = 0$. If $(8m)' = 10m$ then all odd numbers $\leq (14m-1)$ have two representations so that $(10m)' \geq 14m$. But then $\rho(12m+2) = 0$. Hence $(8m)' = 10m+1$. But now $\rho(12m+1) > 2$. Thus we have arrived at a contradiction which shows that the only basis of order 2 containing the element 3 and such that every odd positive integer has exactly two representations as the sum of two elements of A is the set $(0, 1, 3, \ldots, 2n+1, \ldots)$.

PROOF OF THEOREM 6.1:

Let A be any basis of order 2. We must show that all sufficiently large positive integers can be expressed as a sum of four or fewer elements of A without repetitions. If A is one of the two sets $(0, 1, 2, 4, \ldots, 2n, \ldots)$ or $(0, 1, 3, 5, \ldots, 2n+1, \ldots)$ then the condition is obviously satisfied. For A any other basis of order 2 we split the proof into two parts.

First, consider z to be an arbitrary odd positive integer larger than $3x$, where x is the even integer of Lemma 6.3. Then $z-x$ is odd and it is always possible to write $z-x = a_1 + a_2$, where $a_1 \neq a_2$, since A is a basis of order 2. Since $\rho(x) \geq 4$

we must be able to write $x = a_3 + a_4 = a_5 + a_6$ where a_3, a_4, a_5 and a_6 are all distinct. As $(z-x) > 2x$ we may say that not more than one of a_1 and a_2 is less than or equal to x. Now a_3, a_4, a_5 and a_6 are all less than or equal to x. Hence there can be at most one of a_1 and a_2 equal to one of a_3, a_4, a_5 and a_6. We have $z = (z-x) + x = a_1 + a_2 + a_3 + a_4 = a_1 + a_2 + a_5 + a_6$. If the a_i, $1 \leq i \leq 6$, are all distinct then we have two ways of expressing z as a sum of four distinct elements of A. Even if two of the a_i are equal, say $a_1 = a_3$, we may still represent $z = a_1 + a_2 + a_5 + a_6$ as a sum of four distinct elements of A.

It is possible, using a similar argument and using Lemma 6.4 to show that in the case when z is an arbitrary even integer larger than $3y$ we may always represent z as a sum of four distinct elements of A.

Hence by taking 'sufficiently large' to mean greater than the maximum of $3x$ and $3y$ we see that the theorem follows.

If it is known that

$$(6.1) \qquad \rho(n) < \frac{n^{\frac{1}{3}}}{6^{\frac{2}{3}}}$$

then Theorem 6.1 may be proved more easily. Making this assumption, Kelly [13] states that $A^2\left(\frac{n}{2}\right) < \sum_{j=0}^{n} \rho(n)$ for large n. That this statement is not true for all bases of order 2 may be seen by considering the set A: 0, 1, 3, 4, 9, 10, 12, 13, 27, ... which was mentioned previously. Due to the nature of construction of the set A, all positive integers of the form (3^k-1), for all $k \geq 0$, are expressible as a sum of 2 elements of A only as $\frac{3^k-1}{2} + \frac{3^k-1}{2}$. Hence $\rho(3^k-1) = 1$ for all non-negative k.

Thus we are able to find examples of arbitrarily large integers n such that $\rho(n) = 1$. Hence $\sum_{j=0}^{n} \rho(n) = (n+1)\,\rho(n)$ adopts the value 3^k for n of the form (3^k-1). The number of elements of A which do not exceed $\frac{3^k-1}{2}$ is 2^k because we have all possible k-ternary-digit numbers consisting of ternary zeros and ones. Thus $A^2\left(\frac{n}{2}\right) = A^2\left(\frac{3^k-1}{2}\right) = 4^k$ and so $A^2\left(\frac{n}{2}\right) > \sum_{j=0}^{n} \rho(n)$ in this case. A correct statement is

$$(6.2) \qquad A^2\left(\frac{n}{2}\right) \leq \sum_{j=0}^{n} \rho(j) \ .$$

This relation holds for all non-negative values of n. Let $A\left(\frac{n}{2}\right) = \alpha$ so that the elements of A which do not exceed $\left[\frac{n}{2}\right]$ are $0 = a_1,\ 1 = a_2,\ a_3,\ \ldots\ a_\alpha$. By summing any two of these elements we obtain some number j, $0 \leq j \leq n$. Hence each sum contributes to some $\rho(j)$. The contribution is of amount 2 if we form a sum by using distinct elements and is just 1 if the same element is used twice. From the above remarks we conclude that

$$\sum_{j=0}^{n} \rho(j) \geq 2((\alpha-1) + (\alpha-2) + \ldots + 1) + \alpha = 2\,\frac{(\alpha-1)}{2}\,\alpha + \alpha = \alpha^2 \ .$$

Thus we see that $A^2\left(\frac{n}{2}\right) \leq \sum_{j=0}^{n} \rho(j)$. That we cannot have a strict inequality can be demonstrated using the basis $0, 1, 3, 4, 9, 10, \ldots$. Although it may not be true that $\rho(j) < \rho(n)$ for $j < n$ we may say that $\rho(j) < \frac{n^{\frac{1}{3}}}{6^{\frac{2}{3}}}$ for all j values being considered. Thus

$$(6.3) \qquad A^2\left(\frac{n}{2}\right) \leq \sum_{j=0}^{n} \rho(j) < \frac{n^{\frac{4}{3}}}{6^{\frac{2}{3}}}$$

for sufficiently large n, since $\rho(0) = 1$, $\rho(1) = 2$.

Hence $A\left(\frac{n}{2}\right) < \frac{n^{\frac{2}{3}}}{6^{\frac{1}{3}}}$. Let us define $\lambda(n)$ to be the number of representations of n as a sum of four elements of A with at least one repetition. If two representations are distinguishable we count both of them. Now

$$(6.4) \qquad \lambda(n) \leq 6 \sum_{A} \rho(n-2j) .$$

The form $(n-2j)$ makes explicit the fact that we are insisting upon at least one repetition, j being an element of A and $0 \leq j \leq \left[\frac{n}{2}\right]$. Let us suppose that $n-2j = \alpha + \beta$ where α and β are distinct elements of A. Then $n = \alpha + \beta + j + j$. The contribution to $\lambda(n)$ is 12. The factor of 6 outside the summation sign together with the definition of the function $\rho(n)$ allows for this factor. The contribution is less if $\alpha = \beta$, this fact being taken care of by the inequality sign. The number of terms in this summation is obviously $A\left(\frac{n}{2}\right)$ so that we may write

$$(6.5) \qquad 6 \sum_{A} \rho(n-2j) < 6\, A\left(\frac{n}{2}\right) \frac{n^{\frac{1}{3}}}{6^{\frac{2}{3}}} < 6\, \frac{n^{\frac{2}{3}}}{6^{\frac{1}{3}}} \cdot \frac{n^{\frac{1}{3}}}{6^{\frac{2}{3}}} = n .$$

We know now that $\lambda(n) < n$. Now $n = 0+n = 1 + (n-1) = \ldots = \left[\frac{n}{2}\right] + \left(n - \left[\frac{n}{2}\right]\right)$. Also, since A is a basis of order 2, every integer j, $0 \leq j \leq n$, is such that $\rho(j) \geq 1$. Thus we must have at least $2\left(\left[\frac{n}{2}\right] + 1\right) > n$ ways of representing n as a sum of four elements of A. Hence Theorem 6.1 follows.

We now make some introductory remarks before proving Theorem 6.2. Let $B = (b_1, b_2, \ldots b_r)$ be a set of distinct positive integers. Consider any three ordered elements $1 \leq b_i < b_k < b_j$, of such a set. We may write $b_k = b_i + c$, $b_j = b_k + d$ where c and d are positive integers. If the equation $b_i + b_j = 2b_k$ holds we have $b_i + (b_k + d) = (b_i + c) + b_k$ so that $c = d$ which means that the elements b_i, b_j, b_k are in arithmetic

progression. We say that a set B is progression-free if the equation $b_i + b_j = 2b_k$ has no solution with $i \neq j$. Let x be a positive real number and let $B(x)$ denote the maximum number of integers in any progression-free set whose elements are less than x. A theorem of Roth [23-25] states that

$$(6.6) \qquad B(x) = O\left(\frac{x}{\log\log x}\right) .$$

Hence we may write $B(x) < \dfrac{D_1 x}{\log\log x}$ for a suitable constant D_1. Let S be any set of non-negative integers and let T be the set of integers such that each integer of T is representable as a sum of two elements in S in just one way, namely as $2 s_i$, s_i an element of S. If we assume that S is progression-free then so is T because $2(2 s_k) = 2 s_i + 2 s_j$ implies $2 s_k = s_i + s_j$ which holds only for $i = j = k$. More generally, if $B = (b_1, b_2, \dots b_r)$ is progression-free then so is the set $C = (c_1, c_2, \dots c_r)$ where $c_i = \lambda b_i + \mu$ for $\lambda \neq 0$ and $i = 1, 2, \dots r$. If $2c_k = c_i + c_j$ then $2(\lambda b_k + \mu) = (\lambda b_i + \mu) + (\lambda b_j + \mu)$ from which we have $2b_k = b_i + b_j$ if $\lambda \neq 0$. This equation can hold only for $i = j = k$. If $\lambda = 0$ we have $c_i = \mu$ for $i = 1, 2, \dots r$ so that $2c_k = c_i + c_j$ is satisfied by distinct i, j and k. Let A be an asymptotic basis of order 2. Then A is a set of non-negative integers such that every sufficiently large positive integer can be expressed as a sum of two or fewer, and therefore also as exactly two, elements of A. We assume that if an integer is larger than t then it is sufficiently large. Let x be an integer greater than t which cannot be represented as a sum of three distinct elements of A.

Thus we are assuming that we have an asymptotic basis of order 2 which is not a restricted basis of order 3.

Next, consider an element a_p, of A, such that $a_p \le x$. Now $x - a_p \le t$ or $x - a_p > t$. If $(x-a_p) > t$ we must have either $x-a_p = 2a_q$, where a_q is an element of A, or $x-a_p = a_p + a_r$ with a_r in A because A is an asymptotic basis of order 2. We cannot have $x-a_p = a_\sigma + a_\tau$ with σ, τ, and p distinct and a_σ, a_τ in A because if this were so we could represent x as the sum of three distinct elements of A, contrary to assumption. We define an x-chain to be a collection of elements $a_1, a_2, \dots a_k$ in A such that $x-a_1 = 2a_2$, $x-a_2 = 2a_3, \dots x-2a_{k-1} = 2a_k$ where the equations $x-a_e = 2a_1$ and $x-a_k = 2a_m$ with a_e, a_m in A have no solutions. Consider any element a_σ of A such that $0 \le a_\sigma \le x-(t+1)$. For any such element $x-a_\sigma > t$ which implies that a_σ belongs to exactly one x-chain. If x is an element of A then x belongs to exactly one x-chain. Hence every element of A which is less than or equal to x, with at most t exceptions, belongs to exactly one x-chain.

It is easily shown by induction that

$$(6.7) \qquad a_n = \frac{2}{3}(x-3a_1)\left(-\frac{1}{2}\right)^n + \frac{x}{3}, \quad (1 \le n \le k).$$

We see that the elements of an x-chain are all distinct unless $a_1 = \frac{x}{3}$, when all the elements are the same. The number of distinct elements in an x-chain will be called its "length" and will be denoted by k.

Putting $n = k$ in (6.7) we see that since a_k is integral it is necessary that $2^{k-1} \mid (x-3a_1)$. We say that an x-chain is associated with m if $2^m \mid (x-3a_1)$. Thus $k \le m+1$ for $a_1 \ne \frac{x}{3}$. Also we shall have $m \le u = \left[\frac{\log x}{\log 2}\right] + 1$. If $a_1 = \frac{x}{3}$ we put $k = 1$, $m = 0$.

The integer $(x-a_1)$ has only the representation $(x-a_1) = 2a_2$ as a sum of two elements of A because $x-a_1 = a_1 + a_e$ for a_e an element of A would imply $x-a_e = 2a_1$ and a_1 would not be the initial element of its x-chain. Hence the initial elements of all x-chains must form a progression-free set. In particular the initial elements of the x-chain associated with m must form a progression-free set. Consider integers of the form $\frac{x-3a_1}{2^m}$ where a_1 runs over all the initial elements of chains associated with m. This set of integers also forms a progression-free set. Since $0 \leq a_1 \leq x$ these integers lie in the closed interval $\left[-\frac{x}{2^{m-1}}, \frac{x}{2^m}\right]$, of length $\frac{3x}{2^m}$. Let us denote by $\alpha(m)$ the number of x-chains associated with m. Then $\alpha(m) \leq B\left(\frac{3x}{2^m}\right)$. Also the total number of x-chains in $\leq B(x)$.

We are now in a position to prove Theorem 6.2.

PROOF:

By a previous remark we have

$$(6.8) \qquad A(x) \leq t + \Sigma k \leq t + \Sigma (m+1)$$

where the unindexed summations are taken over all x-chains. Now for any m we have $\alpha(m)$ x-chains. Hence $\Sigma m \leq \sum_{m=0}^{u} m\, \alpha(m)$ so that

$$(6.9) \qquad A(x) \leq t + \sum_{m=0}^{u} m\, \alpha(m) + \Sigma 1 .$$

Let us put $v = \left[\frac{\log x}{2 \log 2}\right]$. We may now write

$$(6.10) \qquad A(x) \leq t + \sum_{m=0}^{v} m\, B\left(\frac{3x}{2^m}\right) + \sum_{m=v+1}^{u} m\, B\left(\frac{3x}{2^m}\right) + B(x)$$

Using Roth's theorem [23-25] we are able to write $B(x) \leq \frac{c_1 x}{\log\log x}$ for a suitable constant c_1. Further, since $x^{\frac{1}{2}} \geq \frac{x}{2^m}$ for $m \geq v+1$ we may write

$$(6.11) \qquad A(x) \leq t + \sum_{m=0}^{v} m\, c_1 \frac{3x}{2^m} \frac{1}{\log\log\left(\frac{3x}{2^m}\right)} + \sum_{m=v+1}^{u} m\, B(3x^{\frac{1}{2}}) + \frac{c_1 x}{\log\log x}$$

$$(6.12) \qquad A(x) \leq t + \sum_{m=0}^{v} \frac{3\, c_1\, m\, x}{2^m} \frac{1}{\log\log(3x^{\frac{1}{2}})} + 3x^{\frac{1}{2}} \sum_{m=v+1}^{u} m + \frac{c_1 x}{\log\log x}$$

$$(6.13) \qquad A(x) \leq t + \frac{c_2 x}{\log\log x} \sum_{m=0}^{\infty} \frac{m}{2^m} + c_3 x^{\frac{1}{2}} \log^2 x + \frac{c_1 x}{\log\log x}$$

$$(6.14) \qquad A(x) \leq t + c_4 \frac{x}{\log\log x}$$

where c_2, c_3, c_4 are suitable constants. Our initial assumption, together with (6.14) implies Theorem 6.2.

BIBLIOGRAPHY

[1] Behrend, F. A. "On sets of integers which contain no three in arithmetical progression", Proceedings of the National Academy of Sciences, vol. 32, (1946), pp. 331-332.

[2] Brauer, A. T. "Über Sequenzen von Potenzresten", Sitzungberichte der preussischen Akademie der Wissenschaften, (1928), pp. 9-16.

[3] ———— "Über Sequenzen von Potenzresten II", Sitzungberichte der preussischen Akademie der Wissenschaften, (1931), pp. 3-15.

[4] ———— "On addition chains", Bulletin of the American Mathematical Society, vol. 45, (1939), pp. 736-739.

[5] Braun, J. H. American Mathematical Monthly, vol. 59, (1952), p. 253.

[6] Davenport, H. "The higher arithmetic", (1952), p. 57.

[7] Erdös, P. "On integers of the form $2^k + p$ and some related problems", Summa Brasiliensis Mathematicae, vol. 2, (1950), p. 8.

[8] ———— "Some remarks on number theory", Riveon Lematematika, vol. 9, (1955), p. 48.

[9] ———— "Problems and results in additive number theory", Colloque sur la théorie des nombres, (1955), pp. 135-137.

[10] ——————— and Mirsky, L. Problem set distributed by Mathematical Association of America, (1954).

[11] ——————— and Rado, R. "Combinatorial theorems on classifications of subsets of a given set", Proceedings of the London Mathematical Society, vol. 2, (1952), pp. 419, 438-439.

[12] ——————— and Turán, P. "On a problem of Sidon in additive number theory and some related problems", Journal of the London Mathematical Society, vol. 16, (1941), pp. 212-215.

[13] Kelly, J. B. "Restricted bases", American Journal of Mathematics, vol. 79, (1957), pp. 258-264.

[14] Khinchin, A. Y. "Three pearls of number theory", (1952), pp. 11-17.

[15] Moser, L. oral communication.

[16] ——————— American Mathematical Monthly, vol. 58, (1951), p. 564.

[17] ——————— American Mathematical Monthly, vol. 59, (1952), p. 253.

[18] ——————— "On non-averaging sets of integers", Canadian Journal of Mathematics, vol. 5, (1953), pp. 245-252.

[19] Motzkin, T. S., Ralston, K.E. and Selfridge, J. L. "Minimal overlapping under translation", Bulletin of the American Mathematical Society, vol. 62, (1956), p. 558.

[20] Pall, G. "On sums of squares", American Mathematical Monthly, vol. 40 (1933), pp. 10-18.

[21] Rado, R. "Studien zur Kombinatorik", Mathematische Zeitschrift, vol. 36 (1933), pp. 424-480.

[22] ———————— "Note on combinatorial analysis", Proceedings of the London Mathematical Society, vol. 48, (1945), pp. 122-160.

[23] Roth, K. F. "Sur quelques ensembles d'entiers", Comptes Rendus Academie de Science, vol. 234, (1952), pp. 388-390.

[24] ———————— "On certain sets of integers", Journal of the London Mathematical Society, vol. 28, (1953), pp. 104-109.

[25] ———————— "On certain sets of integers (II)", Journal of the London Mathematical Society, vol. 29, (1954), pp. 20-26.

[26] Salem, R. and Spencer, D.C. "On sets of integers which contain no three terms in arithmetical progression", Proceedings of the National Academy of Sciences, vol. 28, (1942), pp. 561-563.

[27] ———————————————— "On sets which do not contain a given number in arithmetical progression", Nieuw archief voor wiskunde, vol. 23, (1950), pp. 133-143.

[28] Salié, H. "Über Verteilung natürlicher Zahlen auf elementfremde Klassen", Berichte über die Verhandlungen der sächsischen Akademie der Wissenschaften zu Leipzig, vol. 4, (1954), pp. 1-26.

[29] Scholz, A. Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 47, (1937), p. 41.

[30] Schur, I. Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 25, (1917), pp. 114-117.

[31] Swift, J. D. "Sets of covering congruences", Bulletin of the American Mathematical Society, vol. 60, (1954), p. 390.

[32] Utz, W. R. "A note on the Scholz-Brauer problem in addition chains", Proceedings of the American Mathematical Society, vol. 4, (1953), pp. 462-463.

[33] van der Waerden, B. L. "Beweis einer Baudetschen Vermutung", Nieuw archief voor Wiskunde, vol. 15, (1927), pp. 212-216.

[34] ———————— "Einfall und Überlegung in der Mathematik I", Elemente der Mathematik, vol. 8, (1953), pp. 121-129.

[35] ———————— "Einfall und Überlegung in der Mathematik II", Elemente der Mathematik, vol. 9, (1953), pp. 1-9.

[36] ——————————— "Einfall und Überlegung in der Mathematik III", Elemente der Mathematik, vol. 9, (1954), pp. 49-56.

[37] Varnivides, P. "Note on a theorem of Roth", Journal of the London Mathematical Society, vol. 30, (1955), pp. 325-326.

[38] Walker, G. W. American Mathematical Monthly, vol. 59, (1952), p. 253.

[39] Witt, E. "Ein kombinatorischer Satz der Elementargeometrie", Mathematische Nachrichten, vol. 6, (1952), pp. 261-262.